Dotouch
触 点 互 动

Cyber Range Solution

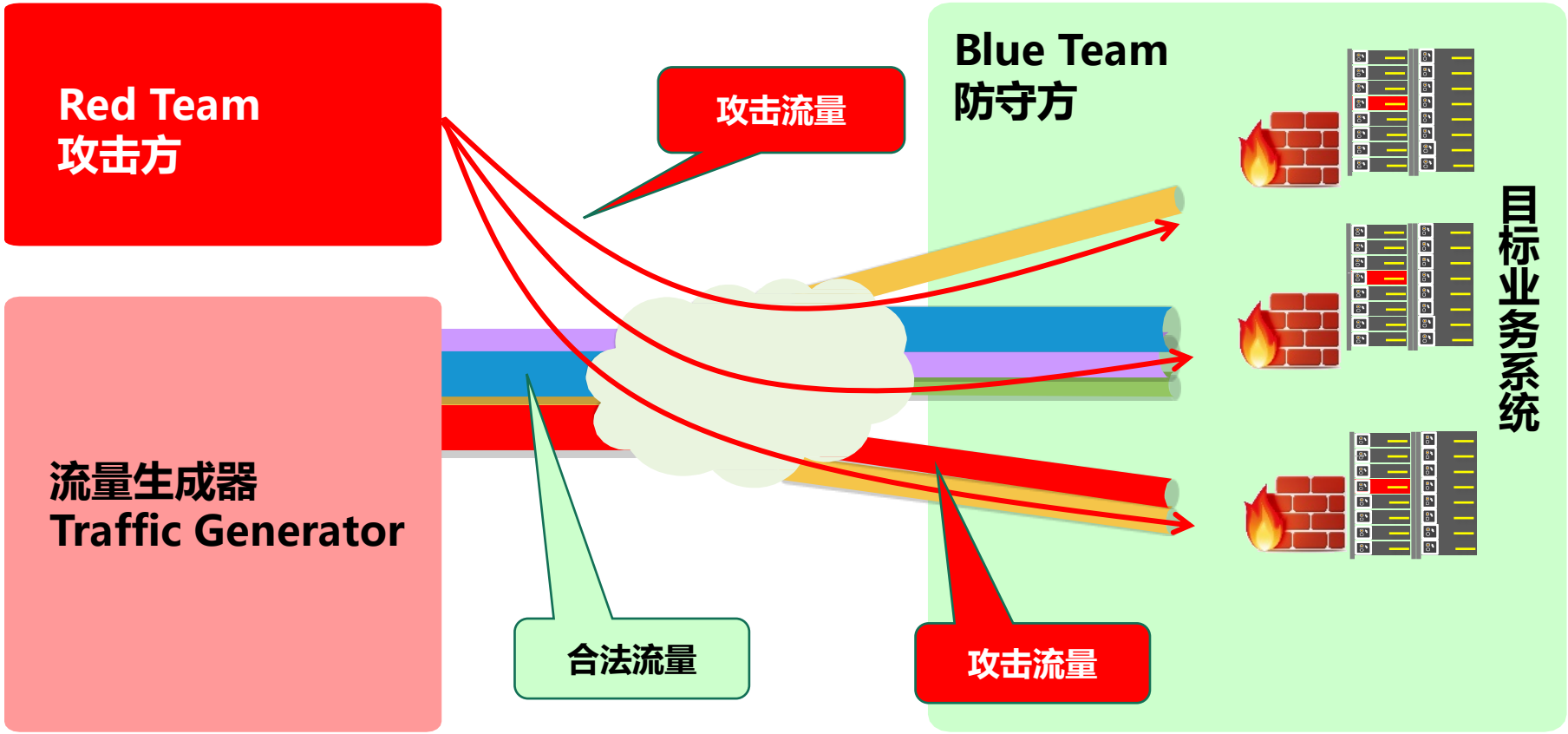
网络攻防电子靶场中的流量发生方案

2022年2月25日

- 背景
- XPRO系列仪表-专业的网络靶场流量生成器
- XPRO构造靶场合法流量的能力
- XPRO构造靶场攻击流量的能力
- XPRO在渗透测试领域的应用场景

构造真实的背景流量是靶场的核心能力

– 真实的网络攻击往往隐藏在海量用户与流量之下，**借助合法流量的掩护，发起攻击**



商业流量发生工具的现状：国外仪表的垄断

专用硬件

仪表类产品都是专用机箱，板卡，很长的供货周期

每隔一个技术周期就要抛弃已有仪表硬件平台

不符合通信云的技术发展趋势要求

功能固化

开发新协议，适配新功能时往往得不到支持

国外供应商对国内需求相应不及时

国内研发和创新的技术成果不能及时得到仪表支持

价格昂贵

动辄百万数量级的采购成本，服务成本奇高

租用成本也非常昂贵

增加协议也要增加软件采购成本

依赖国外厂商

主要依赖思博伦和IXIA 2家公司

存在政治和政策风险

中兴和华为事件影响还未消除，仪表也是被美国禁运禁售对象

涉密项目无法使用国外工具

开源流量发生工具的现状

Dotouch 触点互动

种类繁多

- 很难评估哪种开源软件适用哪种场景
- 每隔一个技术周期就要淘汰一批开源工具，原有技术技能就需要重新积累
- 很多工具不符合国内的法规要求

维护的挑战

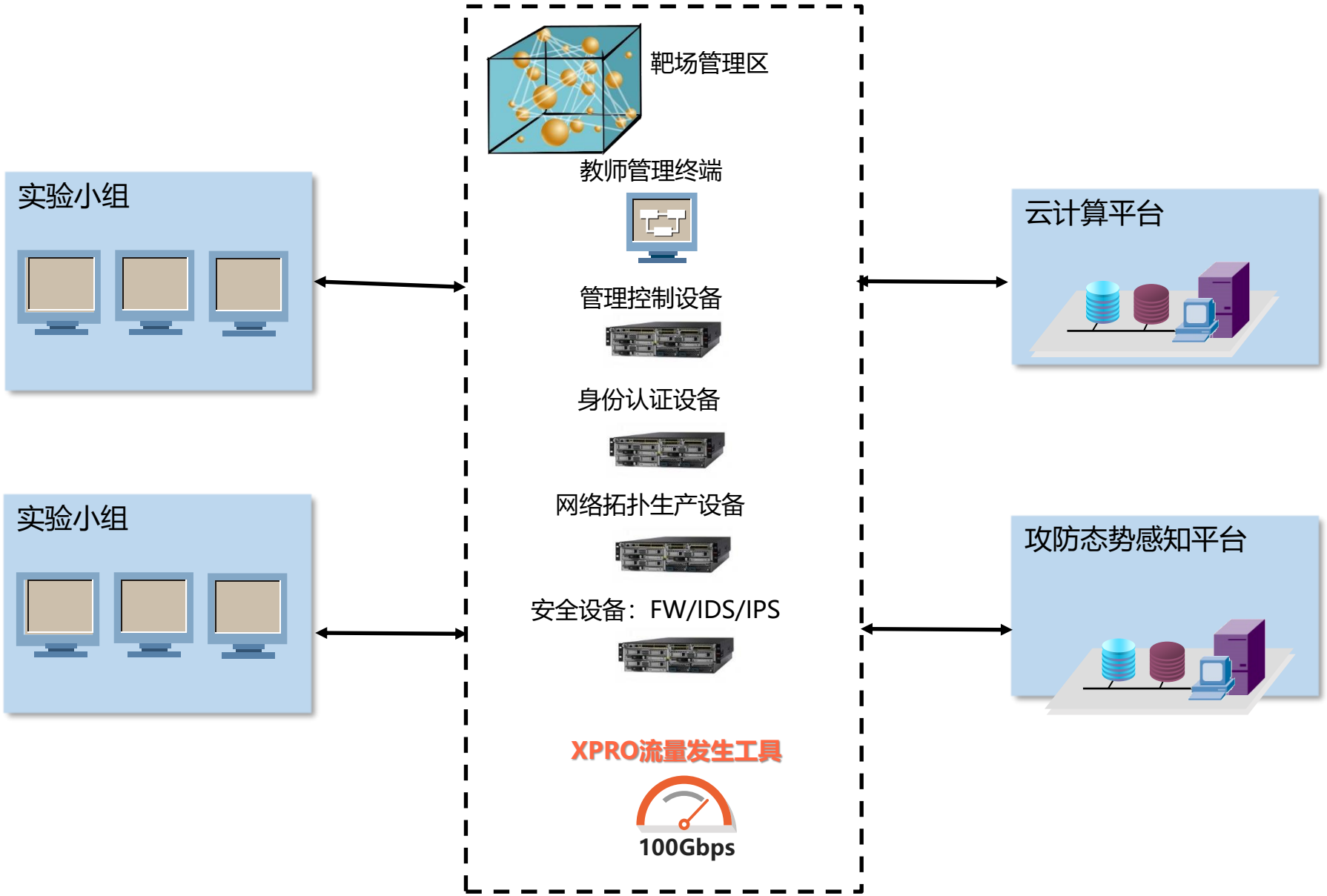
- 只有简单的Github发布文档，没有详细的手册和支持服务
- 测试人员编译和运行Github代码的能力有限，耗费大量精力做重复工作
- 工具Bug修复没有时间承诺
- 工具发展的Roadmap没有承诺

性能挑战

- 大量开源工具的性能未作调优
- 性能参数和硬件的关系需要测试人员自己花时间去测试和摸索

- 背景
- XPRO系列仪表-专业的网络靶场流量生成器
- XPRO构造靶场合法流量的能力
- XPRO构造靶场攻击流量的能力
- XPRO在渗透测试领域的应用场景

网络靶场方案中集成的流量发生工具



XPRO系列高性能流量仿真测试平台

■ 支持靶场模拟移动网场景下的流量仿真

产品定位：高性能4~7层协议仿真

TCP/UDP	HTTP/HTTPS	FTP
DNS over TCP/UDP	IPSec/国密SM1~SM4	L3~L7 Attack
L7 Stateful Replay	IPv4&IPv6 Dual Stack	Others

XPRO NetworkSimulator

XPRO NetworkSimulator是基于Intel DPDK+自研高性能模拟协议栈的高性能网络协议仿真测试平台。

基于高性能模拟协议栈及应用层协议仿真模块，XPRO NetworkSimulator可提供真实和完整的4层状态机制，如TCP连接的建立与拆除、窗口滑动机制、分段自动重传机制，单台双路服务器可输出100Gbps的仿真流量，支持1G，10G，25G，40G，100G接口，支持接口混插。

支持通用应用层标准协议与非标准私有应用协议，如HTTP/HTTPS/FTP/DNS/TCP/国密等，同时可通过带状态的7层回放功能，支持仿真如QQ、微信、迅雷等非标准应用。

产品定位：高性能网络数据包回放

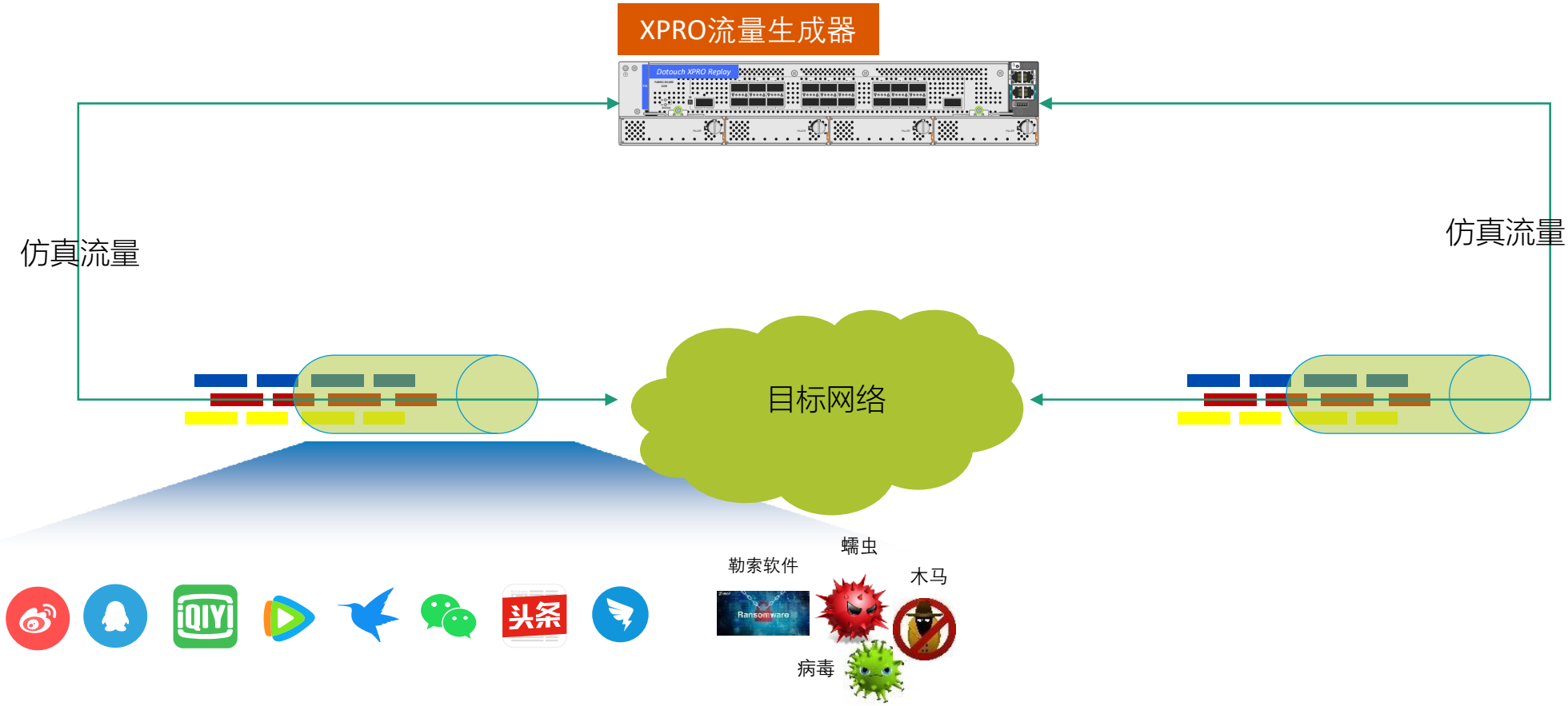
大文件回放	原速回放	GTP封装 Support
多业务按比例混合回放	EPC多信令关联回放	Tunnel Support (GRE/VxLAN)
时延测量/丢包率统计	IPv4&IPv6	Others

XPRO Replay

XPRO Replay是基于Intel DPDK+自研高性能包回放引擎的高性能弱状态网络数据包回放测试平台，支持面向移动网络核心网网元（4G EPC网元，5G核心网网元、IMS等）的测试场景及其他网络设备（汇聚分流设备，DPI等）的测试应用。

XPRO Replay是专门为高性能，高压力，弹性扩展需求的客户所量身定做的解决方案产品，单台双路服务器（三代2690系列CPU）可输出200Gbps的测试流量，支持1G，10G，25G，40G，100G接口，支持接口混插。

XPRO的核心能力



- 支持模拟仿真现实网络中各类协议/应用的流量，如网页浏览，微信，QQ，迅雷等应用产生的流量
- 支持模拟仿真各类网络攻击行为，如DDoS，木马，蠕虫，病毒、勒索软件、SQL注入等攻击行为
- 高性能，单台设备支持100Gbps以上性能，可集群部署，输出超大规模流量

基于X86通用架构的软件化测试工具

Dotouch 触点互动

Before Xpro:

- 专用硬件
- 价格昂贵

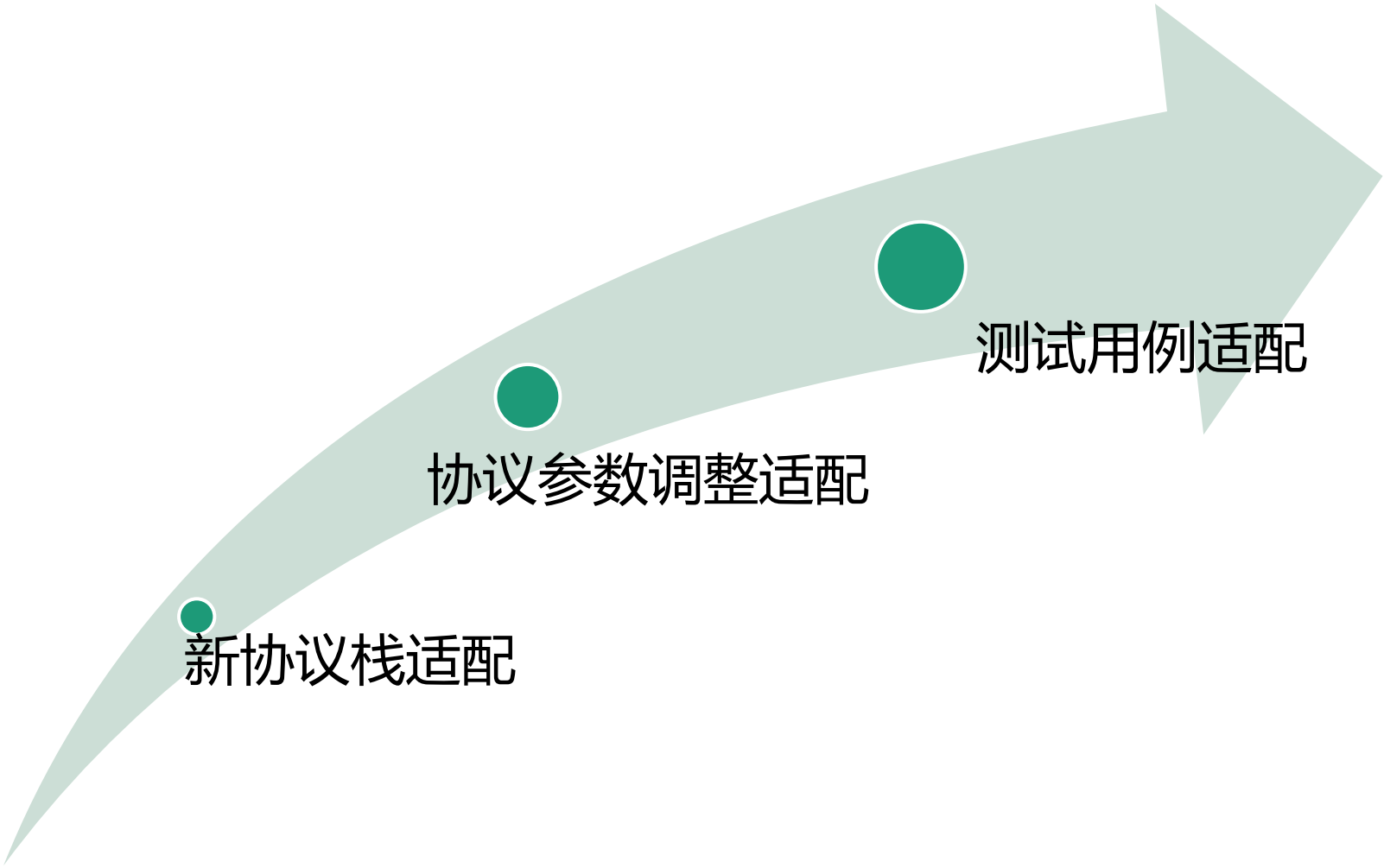
With Xpro:

+

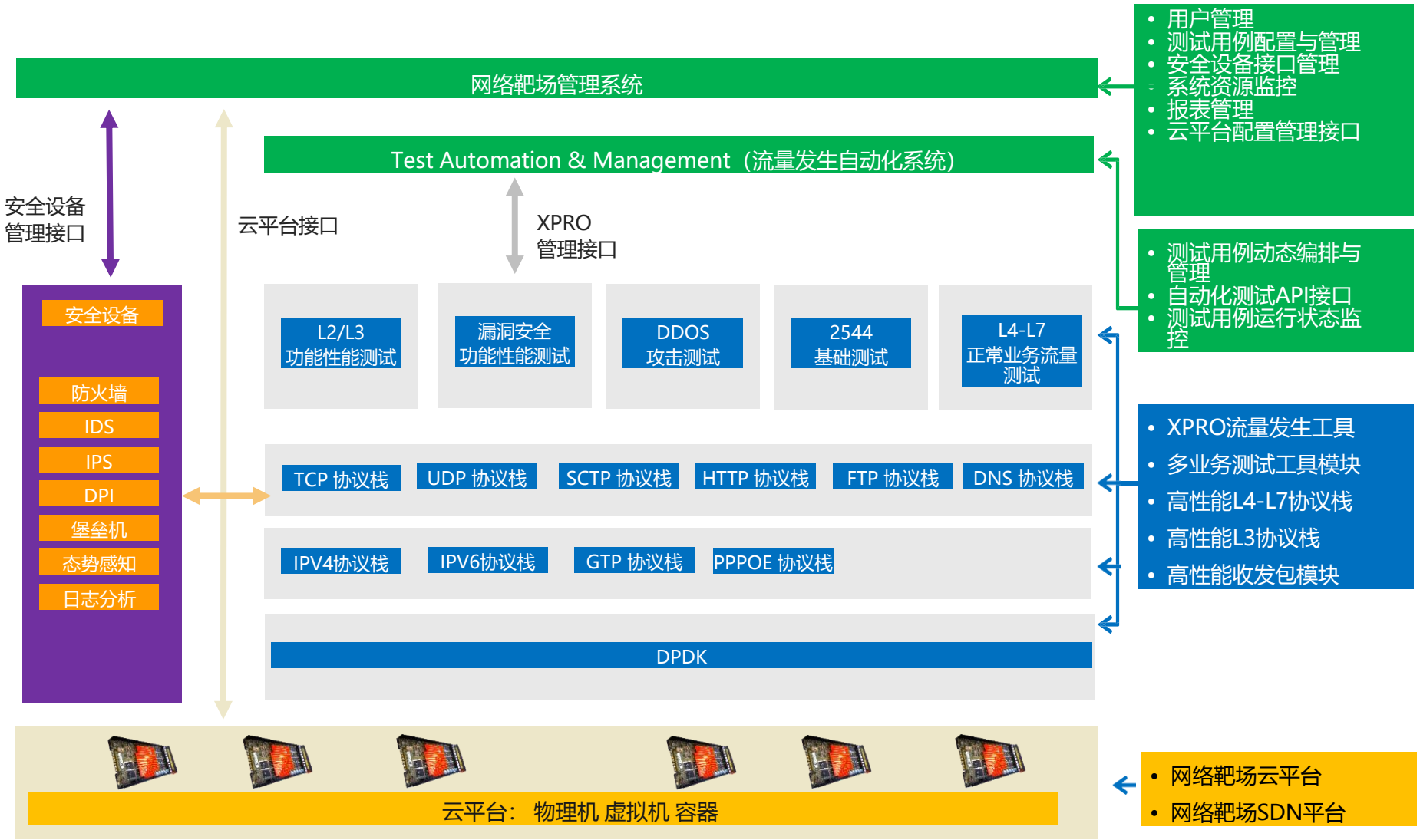
- 基于通用X86架构，更低的硬件成本
- 基于intel DPDK高性能包处理平台，单机/业务板高达200Gbps的发包速率
- 百万级新建连接性能
- 千万级并发连接性能
- 支持10GE/25GE/40GE/100GE各种网络接口
- 支持云化弹性部署 可部署在网络靶场的云平台之上
- 客户端流量仿真和服务端流量仿真可以部署于2台独立服务器之上

快速按需开发定制流量生成方案

Dotouch
触 点 互 动



XPRO与网络靶场的深度集成



- 背景
- XPRO系列仪表-专业的网络靶场流量生成器
- XPRO构造靶场合法流量的能力
- XPRO构造靶场攻击流量的能力
- XPRO在渗透测试领域的应用场景

强大的协议/应用仿真支持能力

Dotouch 触点互动

- **标准协议/应用的仿真**
  - TCP
  - UDP
  - HTTP/HTTPS
  - FTP
  - DNS
  - SMTP/POP3
  - RTSP（在线视频流媒体）
- **非标准协议/应用的仿真**
  - IM类: 微信、QQ、米聊等
  - 下载类：迅雷、eMule，uTronet等
  - ERP：金蝶ERP、用友ERP等
  - 视频类：腾讯视频、各类短视频应用、爱奇艺、网易视频等
  - 办公类：office365、钉钉等
  - 社交类：新浪微博、腾讯微博等
  - 新闻类：今日头条、百度新闻等
  - 游戏类：绝地求生、英雄联盟等
  - 应用商店：苹果应用商店、谷歌应用商店、华为应用市场及其他应用市场等
  - 其他各类私有协议/应用

协议栈维度的仿真能力体现

Dotouch 触点互动

应用层
表示层
会话层

- 支持仿真主流常用标准协议/应用（HTTP/FTP/DNS/RAW etc.），支持协议参数/特性自定义
- 支持HTTPS高性能仿真测试（TLS 1.2）
- 支持基于标准加密套件的IPSec VPN高性能仿真测试，支持加密算法套件自定义
- 支持基于国密SM1~SM4加密套件的高性能仿真测试，支持加密算法套件自定义
- 支持业务响应时间配置 (think time)
- 支持单连接业务数配置
- 支持基于TCP协议栈的7层业务回放，仿真私有应用/协议（QQ/Webchat etc.）
- 支持多业务按模型混合仿真

传输层

- 支持标准的TCP协议栈
- 单机支持超过3,000,000新建，数千万级并发
- 支持负载模型配置（爬坡时间，稳定时间，下坡时间），支持基于时间的负载模型
- TCP响应时延配置
- TCP连接保持时间配置
- TCP窗口大小配置
- 支持TCP Testing Turbo Mode

网络层

- 支持IPv4 & IPv6 双栈
- 支持IP TOS & DSCP 配置
- 支持模拟千万级用户
- 支持延迟测量
- 支持IP分片，支持分片大小、最多分片数量配置

数据链路层

- 支持802.1Q

物理层

丰富的应用层流量的仿真特性（部分）

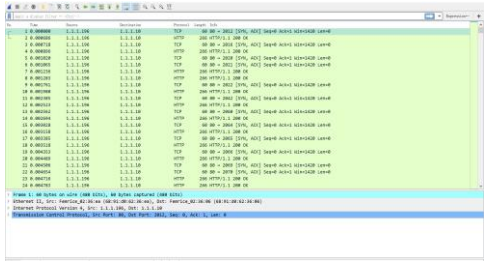
Dotouch 触点互动

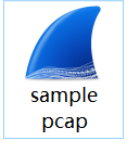
- **HTTP/HTTPS**
  - HTTP Method可配置，支持Head 、Get、Post
  - HTTP header 可配置，可配置标准、非标准头部字段
  - HTTP Client提交内容可配置，可自定义提交内容
  - 支持Host、URI变量，批量生成海量Host与URI
  - 支持HTTP Response Status Code（200 OK，404 Not Found）
  - 支持HTTP Response 内容可编辑，可随机生成指定大小的载荷内容，也可加载指定文件作为响应内容
  - 支持HTTPS加密算法套件自定义
- **FTP**
  - 支持Port mode
  - 支持Passive mode
  - 支持大文件上传与下载
- **DNS**
  - 支持DNS over TCP
  - 支持DNS over UDP
  - 支持IP & 域名对应关系文件批量导入
- **TCP/UDP**
  - 支持基于TCP的裸流应用
  - 支持基于UDP的裸流应用
  - TCP滑动窗口设置
  - TCP会话关闭方式设置

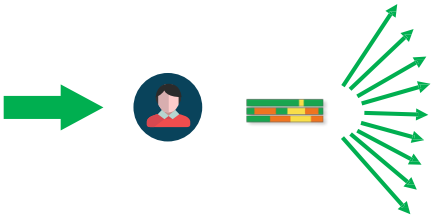
全面支持私有协议/应用的仿真

支持带4层状态的非标准应用/协议的仿真生成

- 支持导入PCAP文件，支持Payload在线编辑
- 基于TCP协议栈的有状态回放，XPRO NetworkSimulator自动构建3、4层状态信息
- 基于单一样包的海量用户复制，支持千万级用户规模
- 支持多业务样包按比例混合回放，构造与现网流量模型一致的混合仿真流量

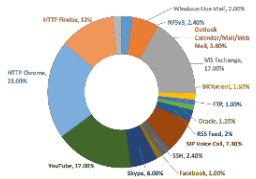


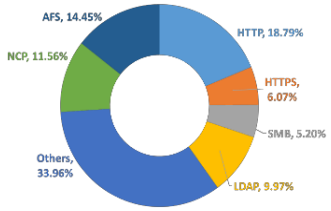


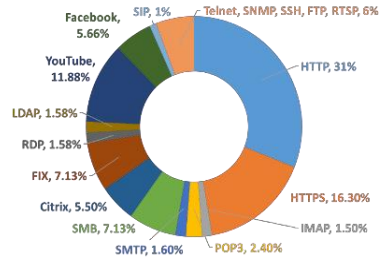


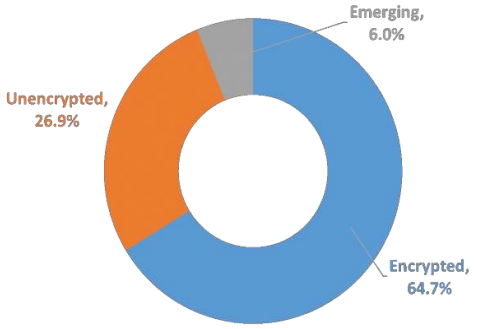
复杂的流量模型构造能力

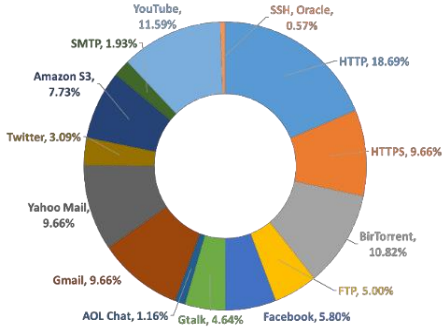
1. XPRO能构造任意的流量模型，模拟不同网络环境下的真实流量构成
2. XPRO内置常见场景的流量模型模板，一键调用
3. XPRO能在测试期间灵活更改流量模型，动态调整流量构成











- 背景
- XPRO系列仪表-专业的网络靶场流量生成器
- XPRO构造靶场合法流量的能力
- XPRO构造靶场攻击流量的能力
- XPRO在渗透测试领域的应用场景

攻击行为仿真 (2019Q3)

Dotouch 触点互动

- **流量生成器内置攻击行为库，攻击方可进行直接调用**

- **对主流攻击行为进行真实复现**
  - Phishing
  - SQL Injection
  - Ransomware
  - Privilege Escalation
  - SCADA Attack
  - …

- **通过特征库的方式进行升级，时刻跟踪最新的攻击手法**
  - APT
  - …

DDOS攻击生成 （Q3发布）

Dotouch 触点互动

应用层

- Reflection/Amplification Attacks（DNS、NTP etc.）
- Application Request Flood
- Other Layer 7 Protocol Floods（SMTP、DNS、SNMP、FTP、SIP、etc.）
- Targeted Application Attacks
- Database Connection Pool Exhaustion
- Resource Exhaustion
- Large POST Requests
- HTTP Get Request Exhaustion
- Slow loris
- Slow POST
- Slow Read
- Mimicked User Browsing
- HTTPS Encrypted Attacks （any HTTP attack，Slow Loris，Slow POST，etc.）

表示层

- SSL Exhaustion

会话层

传输层

- TCP SYN Flood & TCP Reflection Attack
- UDP Flood & UDP Reflection Attack
- TCP Spoofed
- TCP Connection Exhaustion
- IPSec Flood（IKE/ISAKMP Association Attempt）
- Slow Transfer Rate
- Long lived TCP Sessions

网络层

- IP Flood
- IP Frag
- ICMP Flood
- ICMP Frag
- Smurf Attack

数据链路层

物理层

基于CVE漏洞的应用层DDOS攻击生成 （Q3发布）

Dotouch 触点互动

- **基于CVE漏洞库的攻击流量发生**
  - 以流量回放形式进行漏洞攻击的模拟
  - 支持双臂测试的拓扑，对IDS/IPS/WAF/态势感知等安全设备进行测试
  - 支持混合正常业务流量和攻击流量，进行对现网环境的逼真仿真
  - 支持高性能的流量工具，同时混合高性能的混合畸形包攻击，DDOS攻击和漏洞攻击
  - 支持攻击后的逃逸流量发生
  - 可以用于网络靶场的攻击发生和攻防演练
- **CVE漏洞库的攻击流量构造来源**
  - 基于CVE公告的实验环境重现攻击并捕捉攻击流量
  - 业界联盟合作攻击工具共享
  - 网络协议模糊测试中的漏洞发现过程录制

147542	CVE-2019-9655	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190310)
147543	CVE-2019-9656	Candidate	An issue was discovered in LibOFX 0.9.14. There is a NULL pointer dereference in the fu	MISC:https://github.com/TeamSeri0us/pocs/tree/	Assigned (20190310)
147544	CVE-2019-9657	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190310)
147545	CVE-2019-9658	Candidate	Checkstyle before 8.18 loads external DTDs by default.	MISC:https://checkstyle.org/releasenotes.html#Re	Assigned (20190310)
147546	CVE-2019-9659	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190310)
147547	CVE-2019-9660	Candidate	Stored XSS exists in YzmCMS 5.2 via the admin/category/edit.html "catname" paramet	MISC:https://github.com/yzmcms/yzmcms/issues	Assigned (20190310)
147548	CVE-2019-9661	Candidate	Stored XSS exists in YzmCMS 5.2 via the admin/system_manage/user_config_edit.html	MISC:https://github.com/yzmcms/yzmcms/issues	Assigned (20190310)
147549	CVE-2019-9662	Candidate	An issue was discovered in JTBC(PHP) 3.0.1.8. Its cache management module is flawed.	MISC:https://github.com/jetiben/jtbc/issues/9	Assigned (20190310)
147550	CVE-2019-9663	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190310)
147551	CVE-2019-9664	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190311)
147552	CVE-2019-9665	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190311)
147553	CVE-2019-9666	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190311)
147554	CVE-2019-9667	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190311)
147555	CVE-2019-9668	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190311)
147556	CVE-2019-9669	Candidate	** RESERVED ** This candidate has been reserved by an organization or individual that	will use it when announcing a new security proble	Assigned (20190311)

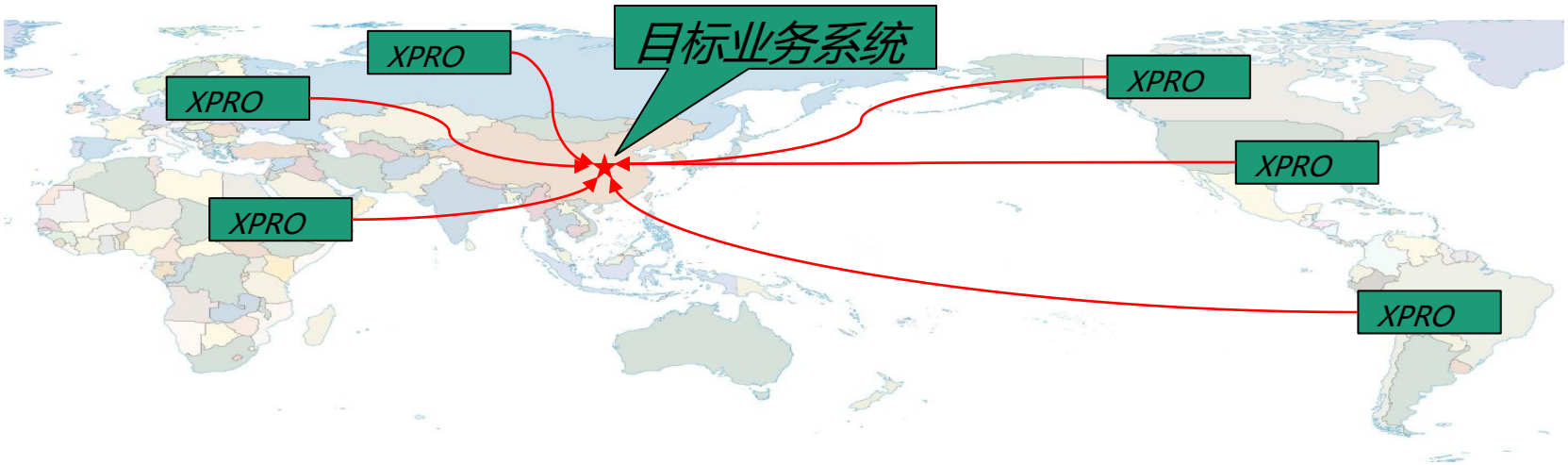
自定义畸形流量的生成

- **基于协议栈的报文自定义编辑**
  - 可以用于网络协议的模糊测试
  - 支持TCP协议，UDP协议之上的数据包根据现场自定义规则进行修改
  - 支持修改TCP协议会话过程中任意报文
  - 自定义规则包括：触发条件；动作；协议；
    - 允许协议类型与字段自定义
    - 触发条件：IP五元组，协议字段，特定数据包偏移位的特征值，支持与/或/非复杂组合逻辑
    - 动作：更改数据包的特定位置的数值，并支持数据步长变化，据数据集合进行更改
- **PCAP回放数据包的自定义包构造**
  - 支持图形化的PCAP数据包改包编辑器
  - 测试人员可以基于已有的PCAP数据流修改其中的数据报文字段，然后进行回放测试
  - 支持大流量高并发的高性能测试环境
- **可用于构造畸形包测试DUT被测设备的安全性，测试可以是双臂拓扑或者单臂拓扑**
  - 畸形包测试规则库采用业界合作方式进行积累和更新
- **混合正常业务仿真流量和畸形流量进行现网环境仿真条件下的安全性测试**
- **可以用于帮助网络靶场构建不同类型的攻击测试**

应用场景1-独立的攻击流量发生系统

XPRO角色定位：

1、XPRO充当专业的攻击流量发生器，用来支撑靶场中攻击测试与渗透测试时打大规模合法流量与渗透测试攻击流量，XPRO可模拟国家级别的超大规模攻击流量



应用场景1-攻击流量发生能力

1. XPRO支持常见攻击（DDoS 、CVE漏洞攻击等）流量的大规模产生

2. XPRO支持全球范围的用户（IP）模拟，模拟攻击行为更贴近现实网络中的攻击行为特征

3. 可部署在国内、国外的公有云服务器之上，支持AWS\Azure\Aliyun的网络接口，支持Vmware虚拟化接口e1000

应用场景2-网络设备的功能与性能验证测试

- IDS/IPS：入侵防御，入侵检测
- Gateway Antivirus：防病毒网关
- Next Generation Firewall：下一代防火墙
- Web Application Firewall：web防火墙
- URL Filter：URL过滤
- Deep Packet Inspection：深度包检测
- Load Balancer/ADC：负载均衡/应用交付
- Network Probe：汇聚分流设备
- Data leakage prevention 数据防泄漏
- APM/NPM：应用/网络性能管理
- Anti-DDoS：DDoS防护设备
- Proxy/Cache：代理/缓存设备or系统
- Content Filter：内容过滤设备/系统
- WAN Accelerator：广域网加速
- IPsec VPN
- SSL Proxy, SSL accelerators：SSL代理，加速

XPRO NetworkSimulator

XPRO Replay

XPRO

应用场景2-网络设备的功能与性能验证测试能力

- **一致性测试**：检验被测设备相关协议的实现是否遵循了协议规范。
- **功能测试**：验证设备是否支持声明的全部功能。（例如：对 协议的支持，过滤功能，流控功能等）
- **性能测试**：通常可以被看成是一种"压力测试"，目的是观察设备在业务压力下的表现。
- **模糊测试**：类似于协议分析，在真实的运行状态下观察协议运行的过程，特别是在有外界干扰和无外界干扰的情况下观察设备的工作状态。

测试内容：
- TCP新建性能测试
- TCP并发性能测试
- 过滤功能测试
- 流控功能测试
- 转发性能测试
- 协议识别准确性测试
- 话单输出性能测试

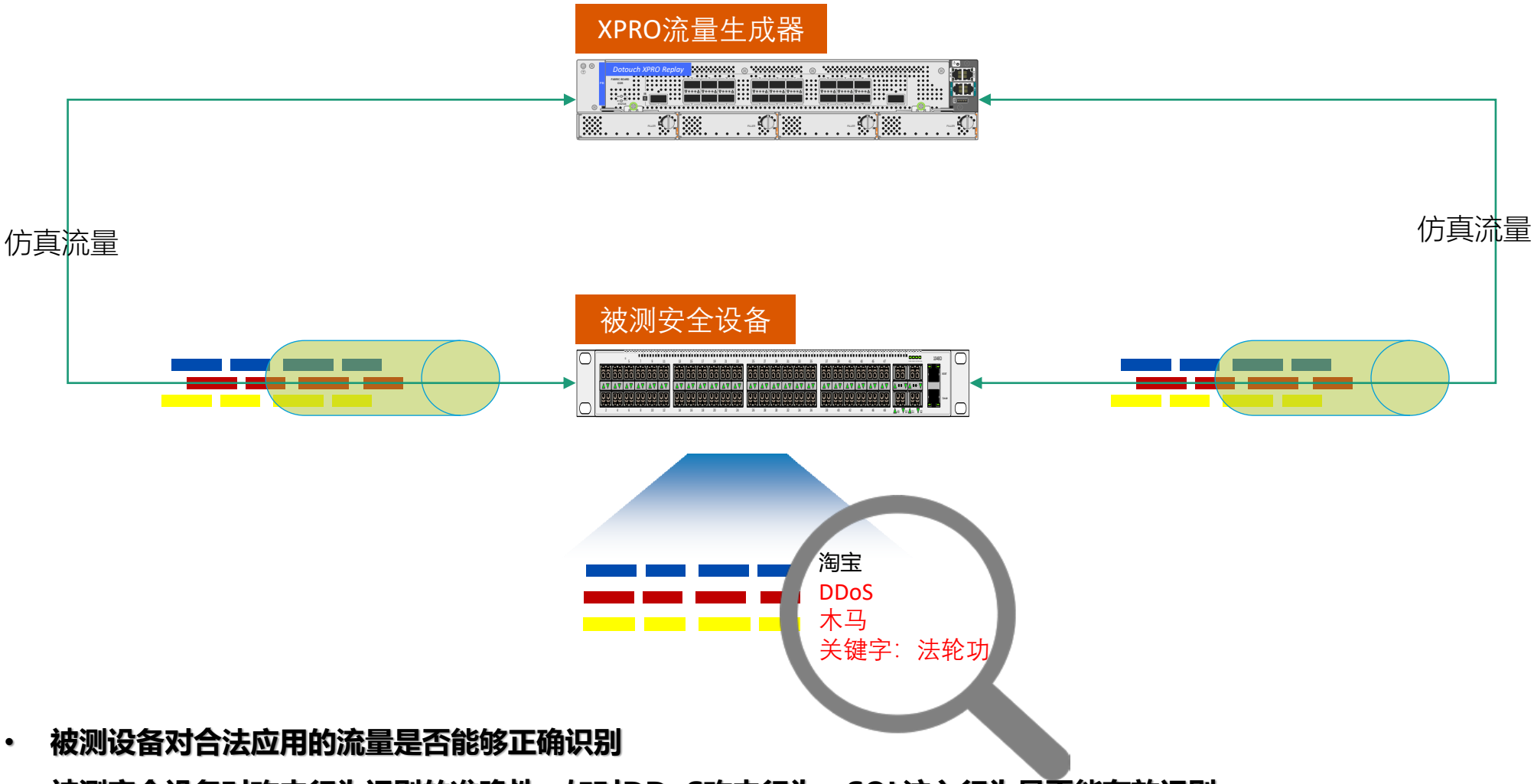
测试内容：
- TCP新建/并发性能测试
- 转发性能测试
- 过滤/流控功能测试
- VPN性能测试
- 协议识别准确性测试
- DDoS防护性能测试
- L7 攻击防护性能测试
- L7 攻击防护准确性测试

测试内容：
- TCP新建/并发性能测试
- 转发性能测试
- 流控功能测试
- 协议识别准确性测试

测试内容：
- TCP新建/并发性能测试
- 包存储性能测试
- 协议识别准确性测试

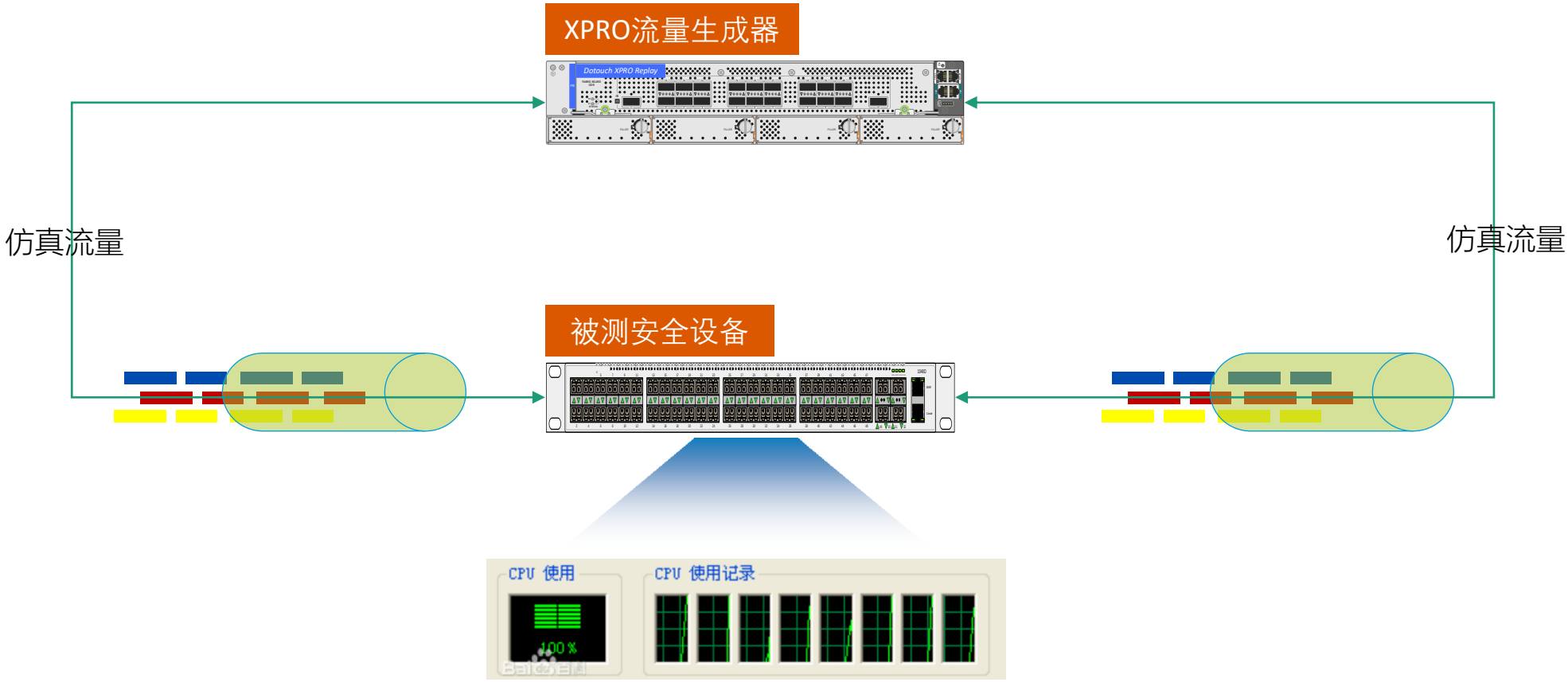
测试内容：
- 标准VPN加解密性能测试
- 国密SM加解密性能测试
- VPN用户接入速度测试
- 转发性能测试
- TCP新建/并发性能测试

应用场景2-对网络设备的功能进行验证与测试



- **被测设备对合法应用的流量是否能够正确识别**
- **被测安全设备对攻击行为识别的准确性，如对DDoS攻击行为、SQL注入行为是否能有效识别**
- **被测安全设备对内容识别的准确性，如对网页内容中涉黄、涉爆、涉恐或指定关键字是否能有效识别**
- **被测安全设备的阻断策略执行的有效性，如对攻击行为、含敏感关键字内容访问的行为在识别后能有效阻断**

应用场景2-对网络设备的性能进行验证与测试

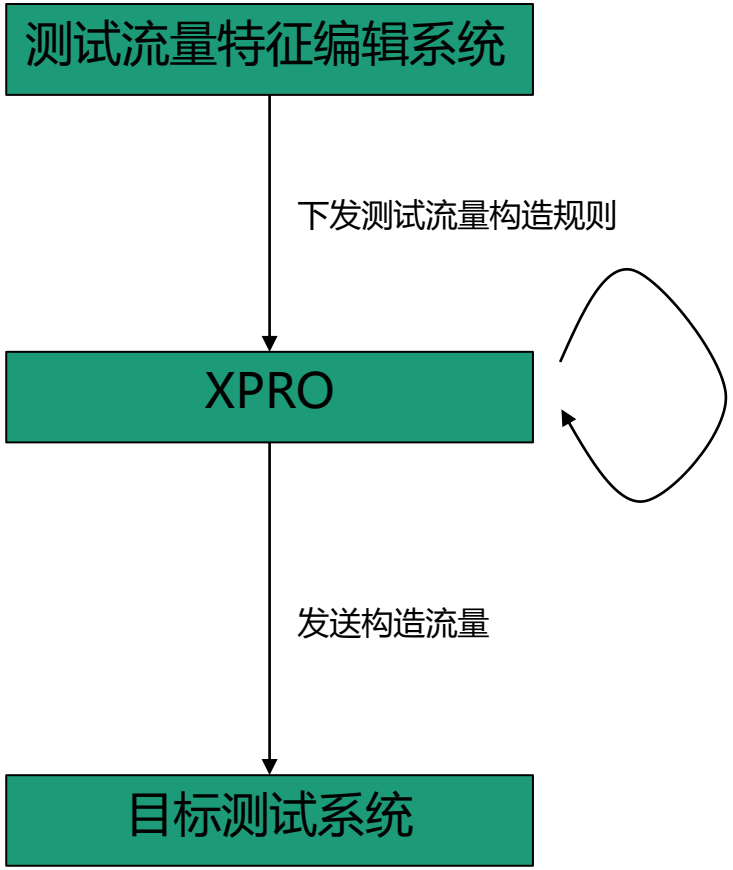


- 测试并验证被测设备在大流量场景下的设备负载，设备是否达到了标称的性能指标
- 测试并验证被测设备在不同流量模型下的设备性能表现
- 测试并验证被测设备在大流量场景下的内容识别、内容过滤、行为阻断功能是否正常

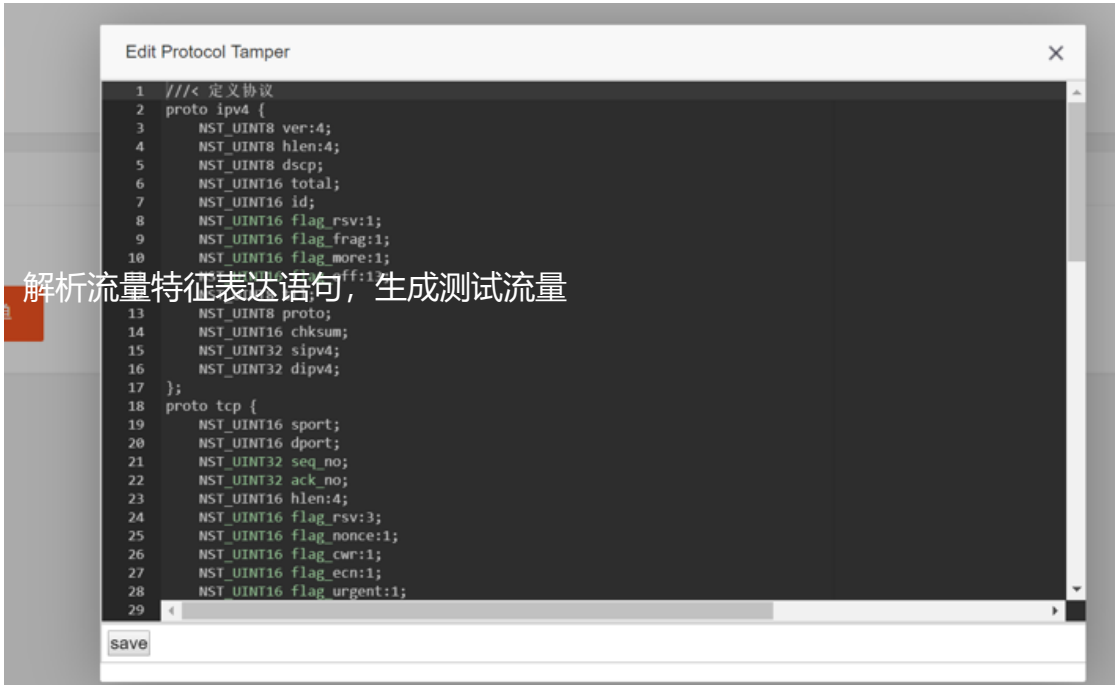
- 背景
- XPRO系列仪表-专业的网络靶场流量生成器
- XPRO构造靶场合法流量的能力
- XPRO构造靶场攻击流量的能力
- XPRO在渗透测试领域的应用场景

应用场景1-渗透测试流量构造

XPRO角色定位：XPRO充当渗透测试流量的构造引擎，接收渗透测试平台下发的流量构造规则，生成一定规模的符合要求的渗透测试流量，同时XPRO也可直接根据内置的攻击特征库，直接按照攻击特征库发起攻击流量



解析流量特征表达语句，生成测试流量



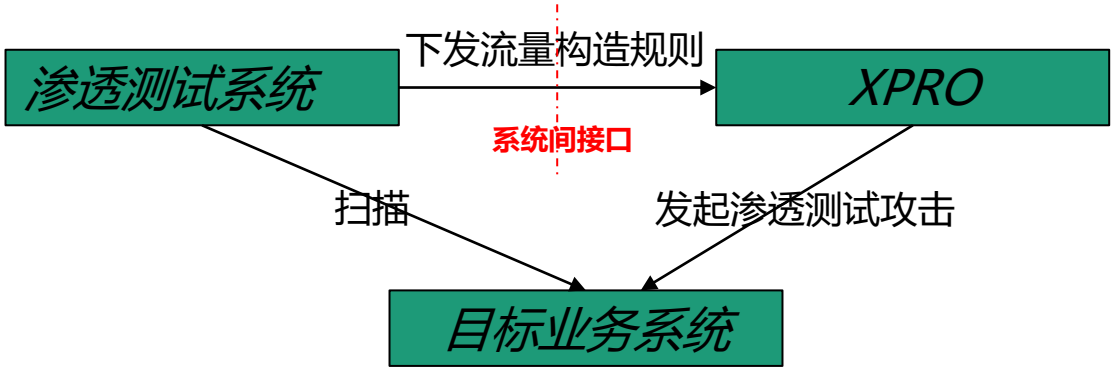
应用场景1-渗透测试流量构造能力

Dotouch 触点互动

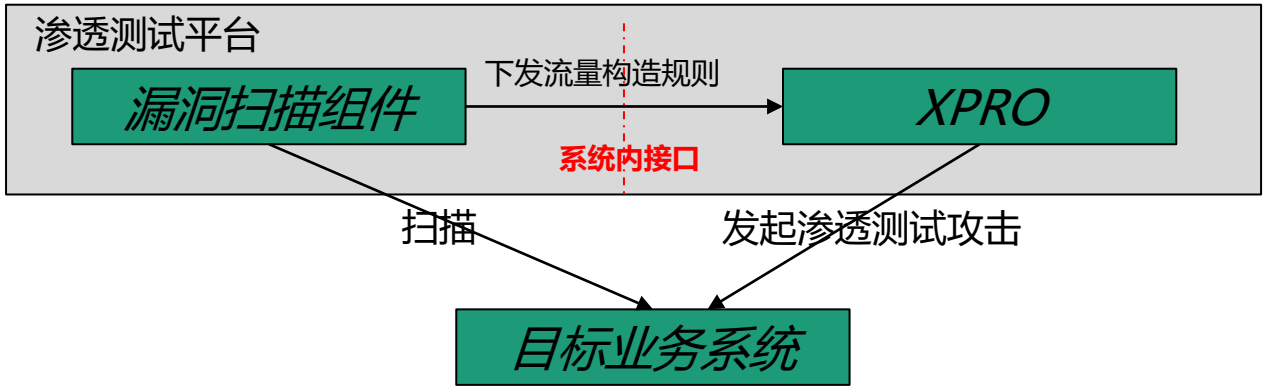
1. 支持构造L2~L7的任意格式的数据包
2. 支持高性能产生构造流量（100Gbps）
3. 支持导入已有的攻击特征样包，XPRO基于该样包进行二次编辑
4. XPRO与渗透测试系统间可通过 API接口对接，接收渗透测试系统下发的构造规则，与渗透测试系统深度集成
5. 支持描述型特征构造语法，用户编辑流量构造特征更友好
6. 支持通过导入脚本的方式导入测试流量特征，方便客户现场工程师测试

应用场景1- XPRO与渗透测试系统的集成方式

方式1：XPRO可作为独立的子系统存在于渗透测试系统中，作为渗透测试系统中的流量发生器，与渗透测试平台自有的渗透测试工具集互相补充



方式2：XPRO作为渗透测试平台的子功能模块，从产品层面整合进渗透测试系统中，充当渗透测试系统的测试流量构造引擎，提高渗透测试系统的流量构造能能力与构造效率



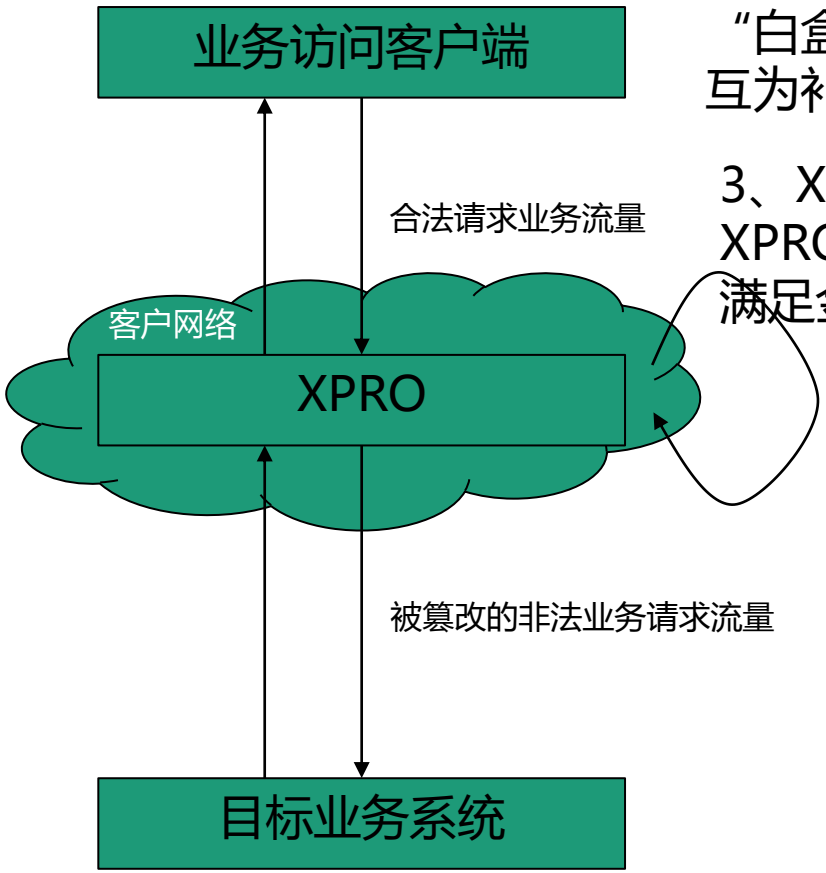
应用场景2-数据流实时篡改

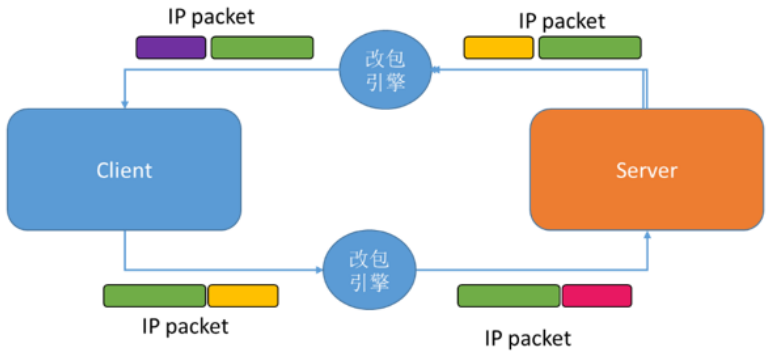
XPRO角色定位：XproN充当实时包篡改系统，对客户的合法业务流量进行解析、篡改后将流量发送至目标业务系统

1、传统的渗透测试是类似“黑盒测试”的渗透测试机制

2、通过XPRO的实时解包与改包能力，对客户端正常的业务请求与服务端响应流量进行篡改，实现类似“白盒测试”的渗透测试机制，与传统的“黑盒测试”互为补充

3、XPRO以串接或并接的方式接入在DMZ区出口
XPRO支持单台双路服务器处理100Gbps测试流量，满足金融、证券等大型客户的测试需求





应用场景2-数据流实时篡改能力

Dotouch 触点互动

1. 支持丰富的网络接口类型，从100M至25Gbps、40Gbps、100Gbps均支持，能接入到绝大部分的网络环境中

2. 支持高性能收发包，即使串接部署在DMZ出口，不会显著增加转发时延，XPRO的转发时延为us级别

3. 支持业务样包抓取、解析、导出

4. 高性能解包与改包引擎，支持自动识别并解析主流应用/协议，单台双路服务器支持高达100Gbps流量处理能力

5. 支持通过界面编辑或导入改包规则，改包规则支持正则表达式，支持多条件关联匹配篡改

应用场景2-XPRO与渗透测试系统的集成方式

Dotouch 触点互动

1. 方式1：XPRO以独立物理机的方式串接部署在测试环境中

2. 方式2：当性能要求不大时。XPRO可直接在虚拟化平台中运行，可与漏洞扫描软件共享服务器资源

3. 在方式1与方式2中，由于业务数据包是在XPRO上进行抓取与解析，因此两种场景下均在XPRO上直接编辑并执行包篡改规则

4. 支持在XPROweb操作界面编辑篡改规则，也可手动直接导入文本形式的流量篡改规则

Dotouch
触 点 互 动

想进一步了解我们的产品?

- 如需试用，请联系我们– market@dotouch.com.cn
- 访问我们的网站了解更多– www.dotouch.com.cn
- 北京触点互动信息技术有限公司
- **Michael - 17771860800**