Dotouch
触 点 互 动

网络安全测试解决方案

1 需求背景

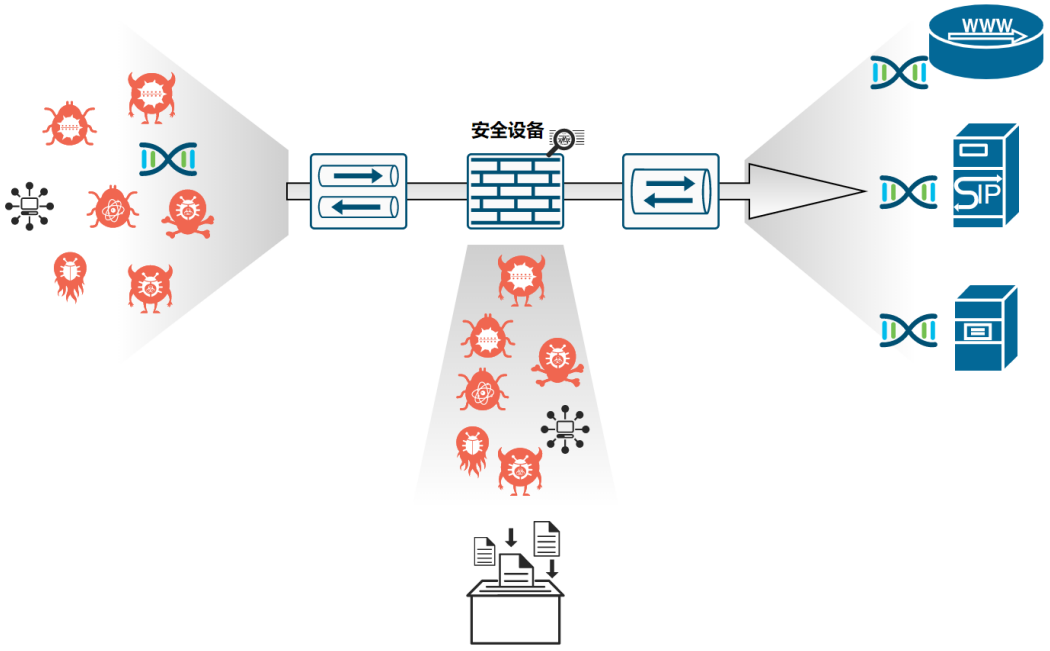
日益庞大与复杂的网络连接了万物，全面云化及 5G 的发展让世界成为一个整体。网络在日益开放的同时，也对各类可见与不可预见的威胁开放了大门，安全上的威胁变的前所未有的紧迫。

在现实网络中，我们部署了种类繁多的安全防护设备与系统，我们希望借助于构建完备的网络安全防护基础设施来帮助我们抵御威胁，然而，随着网络攻击手段与技术的快速演进，庞大的网络安全防护基础设施并不能让我们的网络与应用彻底摆脱威胁，我们需要借助其他技术来帮助我们提升网络安全基础设施的防护能力，让网络变的更安全。

针对上述问题，触点互动推出了业内首个具有完全自主知识产权的网络安全测试解决方案，能对网络安全基础设施设备、整体防护体系进行测试验证，通过仿真各类攻击行为，充分测试与检验网络安全防护设备如 NGFW、WAF、IPS、IDS 的防护能力，以己之矛，攻其之盾，从安全产品开发阶段到现网商用部署，触点互动的网络安全测试解决方案提供全生命周期的测试能力，让网络更安全。

2 业务痛点

网络安全能力的测试依赖于对各类攻击行为的高逼真还原，在当前我们一般通过如下技术手段来实现该目标：



1) 测试人员手动构造攻击报文。此时要求测试人员具备相当的技术能力，考虑到现实网络中攻击手段与技术层出不穷，需要维护一支规模庞大的且具备专业的安全测试能力的技术团队，成本高昂；

2) 测试人员通过蜜罐系统等手段捕获现网的攻击行为及恶意软件样本，再在测试环境中通过回放方式进行攻击行为的再现。该种方式下可以捕获的攻击行为的规模及种类依赖于蜜罐系统所捕获到的攻击行为类型，效率较为低下，且能还原的攻击类型有限；

3) 使用国外品牌的攻击仿真测试仪表进行攻击行为的再现。例如典型的 Spirent CyberFlood 与 IXIA Breaking Point System，但在实际使用过程中，用户普遍反馈国外品牌的攻击仿真测试仪表存在攻击库更新缓慢，对最新攻击行为的跟踪时效性差；另外这类国外品牌的攻击库规模虽较为庞大，但超过 80%的攻击手段与技术在几年前已经出现，并不能真实的反应出当前现网的攻击手段与技术，测试的意义有限；更为致命的是上述品牌的研发技术团队均在国外，所仿真的攻击手段与技术与国内网络中所流行的攻击手段与技术并不一致；

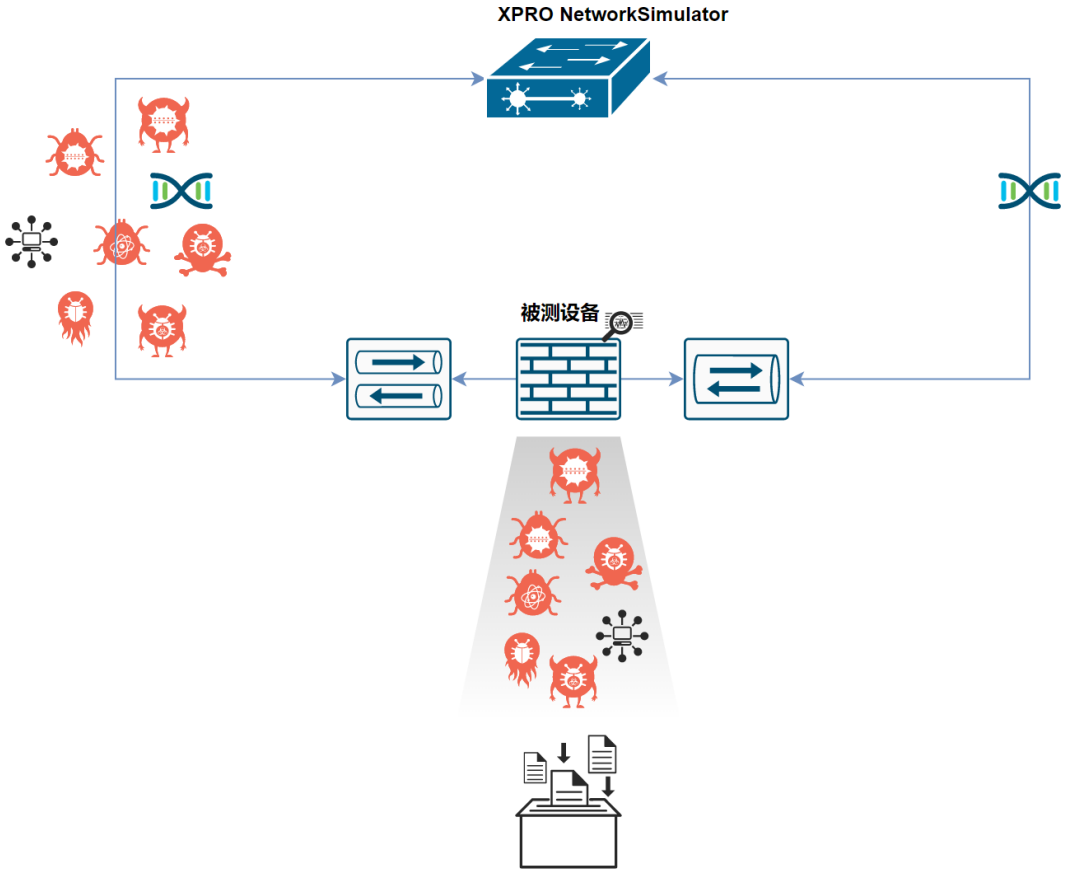
3 解决方案

3.1 方案介绍

触点互动推出的基于 XPRO NetworkSimulator 的攻击仿真测试方案是目前国内首个具有完整自主知识产权的专业攻击仿真测试平台。通过对现网攻击行为的分析与真实再现，借助于 XPRO NetworkSimulator 测试平台，将我们的安全能力赋能给客户，降低用户测试成本、提高用户测试效率。

触点互动基于自有的专业的安全团队，我们实时跟踪最新的安全事件并快速反应，除定期的攻击库更新外，在特殊安全事件发生时，可以通过快速发布更新包的方式实现对热点攻击行为的仿真，如最近出现的针对 Apache Log4j2 漏洞的攻击行为，触点互动在 1 天之内即完成了对攻击行为的分析及攻击库的更新，并快速推送至用户，响应速度远超国外品牌测试仪表。

在实际测试时，触点互动 XPRO NetworkSimulator 测试平台通过仿真指定类型的攻击流量，与合法的流量按照模型混合后送至被测设备，检测被测设备与系统是否能对攻击行为进行有效检测及阻断。



XPRO NetworkSimulator 支持仿真如下类型的攻击行为：

支持仿真的攻击	能力说明
L3-L7 DDoS 攻击，如 Flood 类攻击，畸形包攻击等	支持在线攻击报文构造器，实时构造特定类型的 DDoS 攻击报文，一键还原攻击流量
应用层攻击	支持仿真 SQL 注入、webshell、backdoor、XSS、CSRF、溢出攻击、钓鱼攻击、OS 注入、目录遍历攻击、VOIP 攻击、P2P 攻击等。支持恶意软件库的定期更新及特殊安全事件下的快速更新
APT 攻击	内置集成 NSA 武器库，1：1 还原

工控攻击	支持针对工控网络与应用的 SCADA 类攻击行为的仿真。支持恶意软件库的定期更新及特殊安全事件下的快速更新
恶意软件攻击	内置庞大的恶意软件库、包括僵尸、木马、蠕虫类恶意软件，支持仿真恶意软件的传播、攻击等行为，支持通过 HTTP、HTTPS、SMTP/POP3、FTP 等协议承载恶意软件样本。支持恶意软件库的定期更新及特殊安全事件下的快速更新
协议模糊测试	支持通过 UI 界面构造异常的 L3~4 协议头； 支持脚本驱动的模糊测试引擎，对任意协议字段进行篡改

除支持上述类型攻击行为的仿真外，XPRO NetworkSimulator 支持仿真各类型网络与应用协议，通过灵活设定各类流量的占比，真实还原现网流量特征，帮助用户在实验环境下开展更真实的测试。

支持仿真的协议	能力说明
常规的 L3`L7 层网络与应用协议	IPv4/IPv6/TCP/UDP/FTP/DNS/SMTP/POP3/HTTP/HTTPS/IPSEC/SIP/L2TP/HANDLE/MODBUS/MQTT/LWM2M/OPC UA/CoAP/IEC61850 等

3.2 部署特性

XPRO NetworkSimulator 支持直接部署在 X86/ARM 硬件平台之上以获得最佳的性能表现，支持浪潮、曙光、华为、DELL、HP、H3C 等主流的 X86/ARM 双路或四路服务器。

除支持服务器裸机部署外，XPRO NetworkSimulator 还支持虚拟化部署，支持如下类型的虚拟化平台部署，以满足在私有云与公有云环境下的测试需求：

1) VMware ESXi；
2) KVM；
3) Openstack；
4) 阿里云；
5) 天翼云；
6) 华为云；
7) AWS；

针对网络接口，XPRO NetworkSimulator 支持从 1GbE 到 100GbE 各个规格的物理端口，在云化部署时，XPRO NetworkSimulator 支持 e1000 等主流使用的虚拟接口。

3.3 应用场景

触点互动 XPRO NetworkSimulator 的攻击仿真能力具有广泛的应用场景，如：

1) **安全类产品研发测试场景。**在安全类产品如 NGFW、IPS、IDS、WAF 的研发测试阶段，通过 XPRO NetworkSimulator 的攻击仿真测试能力，真实还原各类型的攻击手段与技术，充分验证产品对各类攻击手段与技术的检测与防护能力。并通过 XPRO NetworkSimulator 构建与现网流量模型一致的流量环境，在实验室即可测试产品在现网流量模型中的各项功能与性能指标。

2) **网络靶场环境集成。**在网络靶场中，XPRO NetworkSimulator 可以作为流量发生器，产生超大规模的背景流量与攻击流量，再现从小规模到超大规模网络中的流量场景，支撑攻防对抗训练与安全技术研究。

3) **网络安全设备选型采购测试。**在用户开展对安全产品的选型采购时，需要借助必要的技术手段对供应商提供的产品型号进行测试与验证，确保其功能与性能符合自身的使用需求。

4) **网络安全防护体系的巡检测试。**在用户完成安全防护体系的建设后，可通过 XPRO NetworkSimulator 仿真各类规模的攻击流量及背景流量，充分验证整个安全防护体系的防护能力，支撑用户评估整个安全防护体系中的

薄弱点，完成安全防护体系的调整、安全策略的优化与加固。并通过常态化的定期巡检测试，实现对网络安全防护能力的持续检测。