Dotouch
触 点 互 动

“护网行动”安全测试解决方案

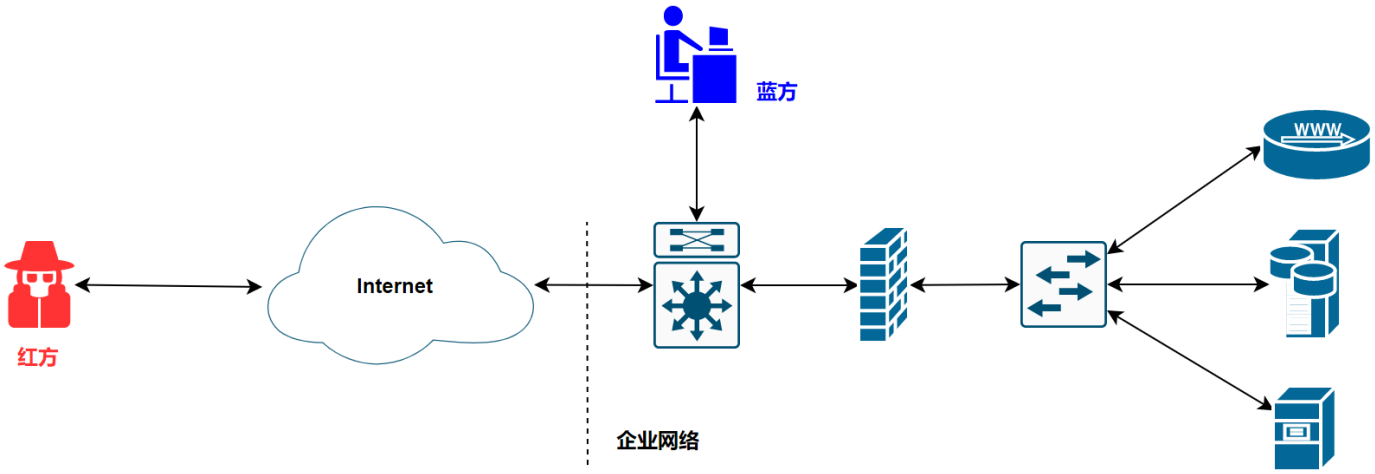
1 需求背景

近几年，随着大数据、物联网、云计算的飞速发展，网络攻击触手已经从企业逐渐伸向国家，国家关键信息基础设施建设也面临着巨大威胁。

在这种严峻的网络安全态势之下，2016 年，公安部会同民航局、国家电网组织开展了 “护网 2016” 网络安全攻防演习活动。同年，《网络安全法》颁布，出台网络安全演练相关规定：关键信息基础设施的运营者应 “制定网络安全事件应急预案，并定期进行演练”。自此，“护网行动” 进入人们视野，成为网络安全建设重要的一环。

2 业务痛点

在 “护网行动” 期间，红方模拟攻击方，向由 “蓝方” 支持的目标业务系统发起模拟攻击，通过这种主动式的模拟攻击检验目标网络与业务的安全性，其测试结果作为重要的技术依据，支撑用户完成对网络与业务安全的优化与加固。



在这种测试模式下，蓝方作为被动防御的一方，需要承受红方不间断的各种攻击，任意一个薄弱环节都可能被红方发现并加以利用，完成攻击动作。这种完全被动防御的方式存在如下问题：

1) 红方的攻击手段与攻击时间是不可预计的，在整个 “护网行动 “期间，蓝方 7*24 小时疲于应对；

2) 蓝方面对攻击手段与技术的多样化，在 “护网行动 “期间，很难针对每一种攻击手段与技术都做好针对性的应对方案，容易后知后觉，待发现异常时往往意味着红网的攻击动作已得逞；

3) 蓝方庞大的网络由不同类型、不同品牌、不同型号的各类网络基础设施设备与业务应用组成，网络规模越大，开放的应用越多复杂，往往意味着可能存在的漏洞越多，进而被红方发现并加以利用；

4) 蓝方整个网络的安全性并不是由单台设备保证的，而是由一系列的设备上部署的策略一起配合完成，例如 WAN 区的安全设备负责流量的访问控制与初步过滤、DMZ 区的安全设备负责应用的攻击检测、LAN 区的安全设备负责完成对可能来自内网的攻击检测与防护、SSL VPN 负责完成远程用户对内网应用的接入访问。整个网络设计复杂，再加上各个设备上叠加的安全策略，容易出现单个设备上均配置了较全面的安全策略，但由于安全防护体系的设计缺陷，导致流量流经的各个节点安全设备上的某条防护策略并没有发挥作用；

通过上面的分析，我们进一步总结为当前的 “护网” 模式存在如下问题：

1) 完全被动的防御疲于应对，发现异常行为时，在极其有限的时间内较难找出适当的技术手段予以应对；

2) 网络可能存在漏洞的点较多，在护网期间，较难都做到很好的兼顾；

3) 网络的复杂性、应用的多样化、各个安全设备上繁杂的防护策略，较难做到协同，容易出现 1+1<2 的情况；

3 解决方案

3.1 方案介绍

针对上述问题，我们需要一套解决方案予以解决，这套解决方案应具备能够在“护网行动“前，模拟”护网行动“中的红方行为的能力，支持蓝方做到有的放矢，不打无准备之仗，避免临场的仓促应对。具体在技术上，具备如下特性：

1) 具备对各类型攻击行为的仿真能力。例如针对 Web 应用的攻击、数据库系统的攻击、文件管理系统的攻击、钓鱼邮件的攻击等等；

2) 具备相当的性能，充分验证网络中可能存在的设备或应用单点性能瓶颈。以应对红方通过大流量直接瘫痪目标网络与应用的目的；

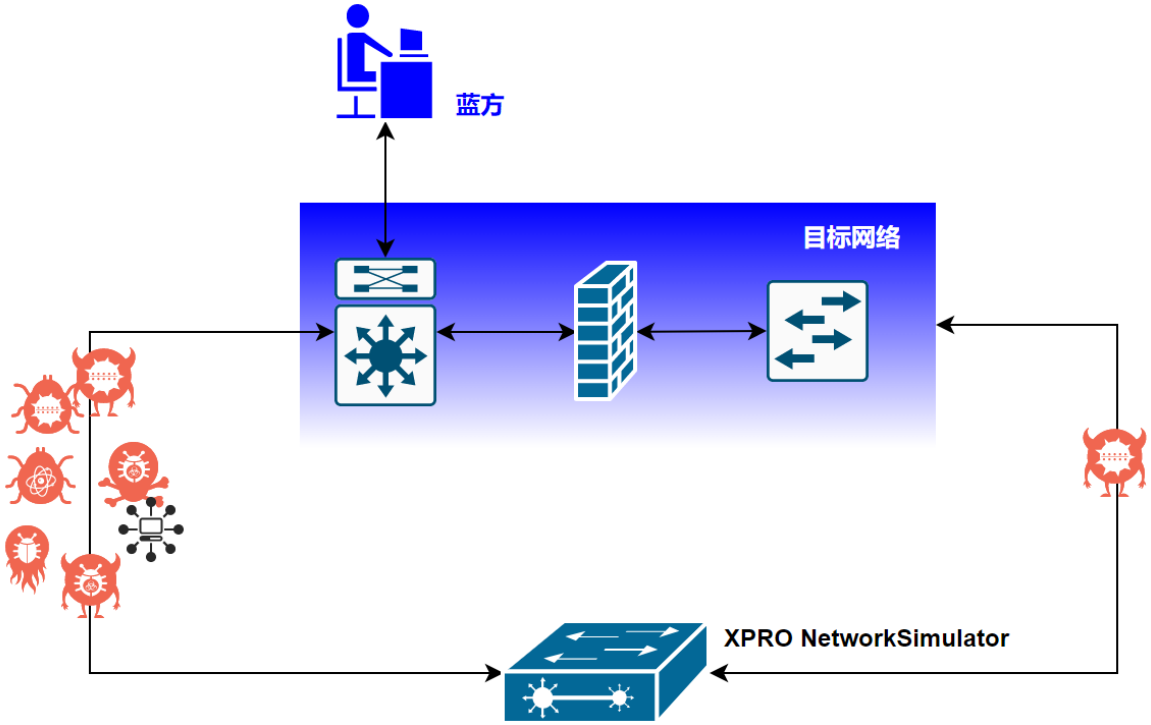
3) 具备对整个网络安全防护体系的测试能力。验证企业网络全路径、端到端的防护能力；

触点互动推出的基于 XPRO NetworkSimulator 的测试方案是目前国内首个具有完整自主知识产权的专业网络仿真测试平台。通过对现网各类型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，在“护网行动“前实现对”护网行动”的预演，支持用户打有准备之仗。

XPRO NetworkSimulator 具备如下仿真测试能力：

支持仿真的协议与攻击	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
特殊场景下的攻击	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
协议异常行为攻击	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
常规协议	IPv4/IPv6/TCP/UDP/FTP/DNS/SMTP/POP3/HTTP/HTTPS/IPSEC/SIP/L2TP/HANDLE/MODBUS/MQTT/LWM2M/OPC UA/CoAP/IEC61850 等

在实际测试时，触点互动 XPRO NetworkSimulator 测试平台通过仿真各种类型的攻击流量，注入至目标网络，检测目标网络是否能对攻击流量进行有效的检测与阻断。



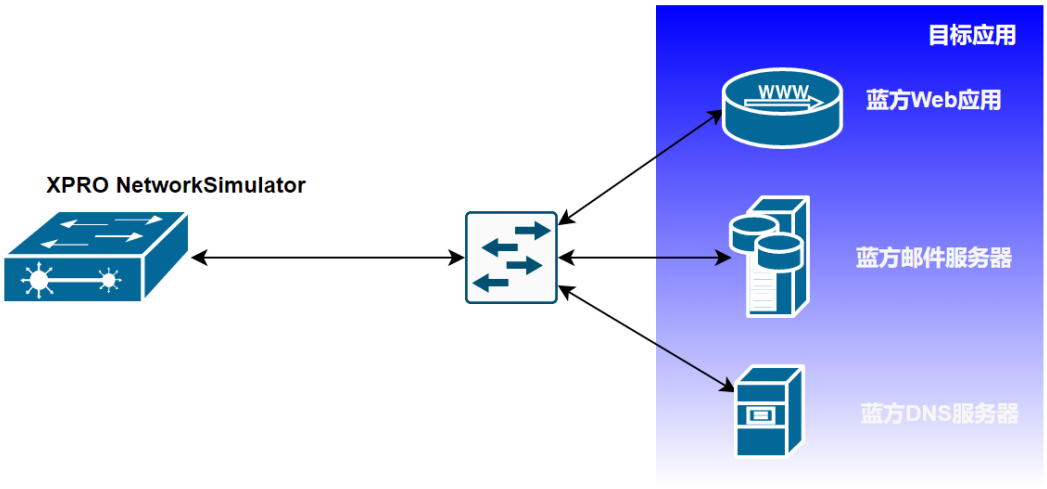
上述测试方式具有如下优点：

1) 可仿真海量的各类型攻击，充分验证蓝方网络是否能对各类型攻击均能有效检测与防护；

2) 可针对整个网络开展性能压测，暴漏性能瓶颈，避免被红方通过大流量瘫痪网络；

3) 既可针对整个网络进行端到端的测试，验证整体系的安全防护能力的有效性，也可支撑开展对单个设备进行针对性测试，

针对蓝方网络中的应用系统，XPRO NetworkSimulator 支持仿真海量的客户端对蓝方的目标应用与邮件服务器、DNS 解析服务器、Web 服务器进行性能压测，支撑蓝方在“护网行动”期间制定有效的限流策略，避免业务系统被大流量瘫痪。



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，以灵活的对蓝方部署在云中的网络与业务进行测试。

XPRO NetworkSimulator 支持如下类型的虚拟化平台部署，以满足蓝方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 价值体现

触点互动的“护网行动”网络安全测试方案具备如下价值：

1) 实现对“护网行动”中红方行为进行预演，支撑用户打有准备之仗；
2) 充分验证用户网络全路径的安全防护能力，支撑用户在“护网行动“前对组网、策略的优化与加固；
3) 支撑用户对单个安全设备进行全面的功能、性能测试验证，评估风险；
4) 开展对用户目标业务系统进行性能压测，支撑用户设计限流策略、进行业务扩容等，规避在“护网行动“中被红网使用大流量瘫痪目标应用；
5) 支撑用户开展常态化的安全测试与演练，不断提升网络安全管理水平；