**信而泰测试方案，助力客户打造网络安全防护“金钟罩”**

**网络安全行业面临的挑战**

据《Cybercrime Magazine》在最近一份报告中称，仅2021年，黑客攻击和各种网络犯罪就给全球经济造成了超过6万亿美元的损失，预计到2025年，此类犯罪每年将使全球经济损失约10.5万亿美元。这样的体量，按规模排名，已经是仅次于美国和中国的世界第三大经济体。而这些犯罪造成的损失明显大于一年内自然灾害造成的损失。这让世界各地的所有公司、中小型企业以及个人，面临着巨大的网络安全挑战。

**网络安全行业发展**

事实上，网络安全不再是一种奢侈品，而是世界上每个个人、企业、组织的迫切需要。在这种背景下，不同国家和地区，各行各业都在大力发展网络安全产业，补充完善当前网络、系统所面临的不足。 根据中国信息通信研究院发布的《中国网络安全产业白皮书》，2020 年全球网络安全市场规模为 1366.6 亿美元，同比增长 8.2% 。2020年我国网络安全产业规模达到1729.3亿元，较2019年增长10.6%。整体来看，网络安全行业发展态势总体良好，技术创新高度活跃，生态建设不断完善，综合实力逐步增强。



**网络安全测试关注点**

在网络安全受到关注之前，不少公司的网络还处于“通与不通”的阶段，能够满足基本上网需求，正常收发邮件，访问一些特定系统（web、ftp等）即可，对安全性并不重视，或者说完全忽视，不会投入过多的人力和资源成本去维护。而随着网络攻击的泛滥，这些系统和网络在黑客，甚至一些学习了IT基础的小白面前变得不堪一击。DDos拒绝访问攻击导致业务系统网络无法访问，勒索病毒会使重要文件无法读取、关键数据被损坏、计算机被锁死无法正常使用，而更隐秘的APT攻击具有极强的隐蔽性和持久性，对目标系统进行持续的信息收集和破坏。

针对这些攻击，安全厂商推出不同的解决方案，DDos、防火墙、IPS/IDS、WAF等等，和路由交换设备一样，这些设备在研发阶段就需要进行各种测试：协议测试、功能测试、性能测试、稳定性测试等2-3层测试仪就能满足的测试需求。而不同的是，**安全设备往往还有更多的关注点，如防火墙领域，比较重要的两个关注参数是新建连接数和并发连接数，除此之外，还有IPS吞吐量、AV吞吐量这些针对不同功能提出来的新关注点。**

**信而泰解决方案**

针对网络安全厂商日益复杂的测试需求，信而泰推出了自研的软件测试平台ALPS，ALPS主要面向4-7层测试，拥有以下7大测试功能：



**7大测试功能大致可分为三类：**

**第一类性能测试，包含session generator组件，主要用于测试设备性能，测试DUT 新建和并发能力。**

**第二类为流量仿真，包含application simulator、client/server simulation、application replay组件，application simulator可以基于内置协议仿真，如http、dns、dns、ftp等常见语音、视频、数据传输协议，其中http协议可以利用client/server simulation组件进行客户端、服务器模拟，进行数据交互，application replay组件则可将真实流量导入进行其他协议模拟仿真。**

**第三类为安全类，包含security、malware、ddosattack组件，security和malware组件用于评估被测设备对安全漏洞、恶意软件和病毒攻击的防护能力，信而泰和专业安全公司合作，提供高达43000+特征库。**

****

Ddos attack组件可用于模拟TCP、UDP、IP、ARP、ICMP、IGMP多种协议中不同的flood攻击类型，以评估被测设备对这些攻击类型的防御能力。



承载ALPS的硬件平台有三个系列：**BigTao系列、Daryu系列和DarPeng系列。**



**Bigtao系列和DarYu系列**除了可以搭载4-7层测试平台ALPS，还可以搭载2-3层测试平台Renix进行协议、功能、性能、稳定性测试。

**DarPeng系列**主要关注更高的性能表现，整机TCP新建370万，并发1亿，吞吐量90G。

除此之外，ALPS测试平台提供了便捷的配置，多样化的统计视图，还提供包括pdf、html、csv多样化格式的报告下载。

