BreakingPoint™ 虚拟版（VE）——虚拟化应用与安全测试解决方案简介

真实世界的测试，帮助企业 IT 部门实现安全弹性

在当今充满网络攻击和动态应用的世界中，企业需要知道自己的网络是否足够安全以应对网络罪犯可能造成的最坏的后果。不过，尽管安全技术开支处于历史最高位，您如何确信自己选择了正确的供应商和安全架构？高保真测试消除了疑虑，通过实测为你带来信心。

通过虚拟化架构和行业通用的硬件平台，IxiaBreakingPoint VE 在弹性部署模式中提供可扩展的真实应用和威胁仿真。利用 BreakingPoint VE 来充分发挥安全投资的效能并优化网络架构，建设你可以依赖的弹性网络。Ixia 经过市场验证的 BreakingPoint 应用现在支持虚拟化，提供经济、弹性且可共享的虚拟化测试功能，这些功能可以在企业分布在各地的网络上快速地部署并扩展。

与高保真且灵活的测试功能同样重要的是 BreakingPoint VE 订阅销售模式，它符合企业按项目投入 IT 运营资金的要求。快速地获得工具、根据项目需求任意缩放，可以部署在任何地方并拥有虚拟化架构的敏捷和简洁性。

- 完整的性能和安全测试
- 优化网络安全设备，例如 IDS/IPS、DLP、UTM、NGFW、WAF、Web 代理

验证针对分布式拒绝服务（DDoS）和其它攻击的防御措施

- 进行设备比拼测试评估
- 为应用和网络实验室添加真实、大规模的仿真威胁
- 在不影响安全性的情况下实现云计算和虚拟网络功能（VNF）承诺的节约
- 通过每月两次的应用和威胁情报（ATI）更新而跟上新应用和威胁的步伐
- 通过在 BreakingPoint VE 中重新使用测试文件而充分利用你在 BreakingPoint 上的投资

恶意与合法流量仿真

被测设备或网络

Metric	Specification	Firewall A	Firewall B	Firewall C
Transactions per Second	10,000	12,243	8,832	N/A
Concurrent Flows (Combined TCP and UDP)	30,000	32,684	57,908	14,618
Average Latency (Microseconds)	5,000	5,114	1,308	235,648
Attacks Blocked (BreakingPoint Security Level 1)	80%	47%	91%	78%
Transactions per Second	8,000	9,268	4,861	N/A

Key: Met Specification | Missed Specification by 5% or less | Missed Specification by more than 5%

根据数据做出决策

ixia

仿真真实的应用和安全攻击

真实的应用

- 370 多个应用协议
- 3,700 多个 Superflows
- 社交媒体、P2P、语音、视频、游戏
- 企业、财务、数据库、Web、移动
- SCADA、存储负载、自定义应用
- 实时更新

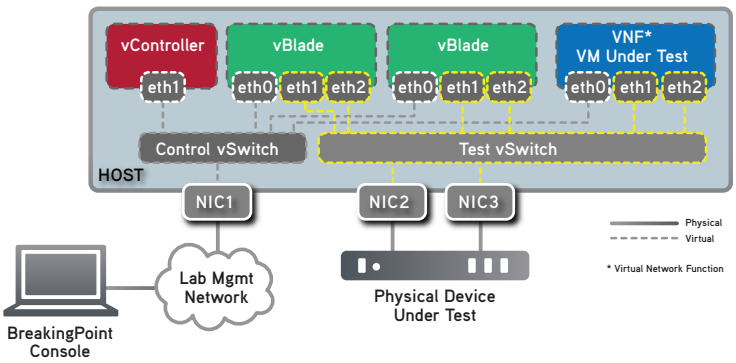
真实的攻击

- 37,000 多种安全攻击
- 7,000 多种现实的安全攻击
- 100 多种逃逸技术
- DDoS 和僵尸网络仿真、自定义攻击
- 研究并提供两周一次的更新

BreakingPoint VE 的组件

BreakingPoint VE 以 OVA 形式提供，在 VMware®管理程序上运行，包括：

- **虚拟控制器——**虚拟化 BreakingPoint 系统控制器
- **虚拟刀片——**虚拟化负载模块（支持最多 8 个端口）



针对物理和虚拟的企业应用与安全测试：

应用测试	网络测试	安全测试
• 应用负载	• 负载均衡	• NGFW
• 应用安全性	• 应用交付	• DDoS 防御
• 服务器容量	• 无线局域网控制器	• 合法拦截
• 呼叫中心	• 防火墙	• DLP
• VoIP	• 路由器/交换机	• IPS
• 数据中心迁移计划	• SBC	• 反病毒/反垃圾邮件
• 视频服务	• IPv6 就绪	• 网络靶场训练

BreakingPoint VE 部署灵活性和可扩展性

单一主机

- 虚拟控制器和虚拟板卡在一台物理主机上
- 一个虚拟控制器可以管理多达 12 个虚拟板卡

可扩展的主机

- 一个主机上的虚拟控制器（有或没有虚拟板卡），可以管理最多 12 个虚拟板卡
- 其它物理主机只包含虚拟板卡