



为防御类型和数量日益增加、危害性不断增强的安全威胁，组织需要通过其网络设备及其功能网络提供高水平的防护与性能。只有通过持续的漏洞检测，网络设备制造商（NEM）、服务提供商与企业才能确定其安全机制可应对最新威胁环境，同时确保网络性能。

安全漏洞使组织处于与以下各项相关的非常真实且代价高昂的风险中：

- 品牌损害
- 服务质量下降
- 服务中断
- 法律风险

安全周边设备（如防火墙、入侵检测与防护系统 [IDS/IPS] 以及网关防病毒与反间谍软件设备）需要持续更新以提供最新防护。Ixia 的测试解决方案可确保您的防御系统紧跟恶意软件与拒绝服务攻击不断发展的步伐。

Ixia 安全测试解决方案包括：

- IxLoad-Attack — 使用持续更新的已知漏洞、恶意软件和高性能分布式拒绝服务（DDoS）攻击库来加强网络防御、验证威胁检测的有效性并报告安全设备的准确性。IxLoad-Attack 还可衡量受攻击时网络安全设备的性能。
- IxLoad-IPsec — 衡量使用 IPsec 加密的 VPN 网关的性能。与 IxLoad-Attack 结合使用时，可对加密链接进行漏洞攻击，模仿多站点和远程工作人员连接。
- IxLoad — 提供全面的语音、视频和数据协议模拟，用于测试真实多重播放情境下的性能。IxLoad-Attack 和 IxLoad-IPsec 是这一基础测试应用程序的可选项。

IP 安全是互联网和企业内部网应用与服务领域的公司必须关注的问题。特定协议和设备旨在提供验证与数据安全，例如与 EAPOL (802.1x)、PPP 和加密技术 (IPsec、TLS 和 SSL) 相关的用户验证。然而，由于安全性、复原能力和稳定性不够，每个协议和设备均可能受到漏洞利用。此外，任何应用程序或系统均有容量限制，并且在该限制时的运转状态经常会成为攻击媒介。

Ixia 提供多个解决方案组合，全面关注网络安全，并模拟各种流量与攻击以探测网络防御中的薄弱环节。

产品	描述
IxLoad-Attack	<ul style="list-style-type: none">• 测试安全设备防御恶意软件与拒绝服务攻击的能力• 利用持续更新的包含成千上万已知漏洞（包括 CVE 索引中的漏洞）的订阅库• 生成线速分布式拒绝服务 (DDoS) 攻击• 测试下一代防火墙、入侵检测与防护系统 (IDS/IPS)、网关防病毒与反间谍软件设备、VPN 网关及其他安全设备
IxLoad-IPsec	<ul style="list-style-type: none">• 对 IxLoad 生成的任何流量（包括攻击与多重播放流量）执行 IPsec 加密• 与 IxLoad-Attack 结合使用，是唯一一款通过加密应用攻击的测试产品，能够采用基于 IPsec 的 VPN 功能来测试安全设备的能力，进而确定内部攻击• 极具可扩展性的解决方案，用于验证 IPsec VPN 网关的性能与功能• 与实施全面 IKE 与 IPsec 协议堆栈的 Ixia 专业化加载模块配合使用，可模拟数以千计的安全网关与客户端及创建数以千计的 IPsec 隧道进行测试
IxLoad	<ul style="list-style-type: none">• 高度可扩展的集成测试解决方案，可评估多重播放网络与设备的性能• 模拟最大范围的语音、视频、数据、存储和基础设施协议• 独特的订阅者模型具有不同的用户组与日程安排，模拟客户的真实使用情况
IxANVL	<ul style="list-style-type: none">• 自动网络和协议验证的行业标准• 使网络设备和互联网设备的开发人员及制造商可验证安全性和认证协议合规性与互通性
IxNetwork	<ul style="list-style-type: none">• 用于展现路由器和交换机性能与可扩展性特点的模拟测试• 包括用于测试与 802.1x、PPP 和 NAC 相关的验证协议的设备

本材料仅作参考之用，如有变更，恕不另行通知。本材料说明了 Ixia 目前将要开发并提供给客户的某些产品、特性和功能的计划。Ixia 仅负责提供与客户之间签订的书面协议中明确提及的产品、特性和功能。