东软 NetEye 入侵检测系统

- **入侵检测 IDS2200-N2202 产品简介**

东软针对网络攻击、违规使用等情况而自主研发的东软 NetEye 入侵检测系统(IDS)采用深度分析技术对网络进行不间断监控，分析来自网络内部和 外部的入侵企图，并进行报警、响应和防范，有效延伸了网络安全防御层次。同时，产品提供强大的网络信息审计功能，可对网络的运行、使用 情况进行全面的监控、记录、审计和重放，使用户对网络的运行状况一目了然；

- **入侵检测 IDS2200-N2202 硬件配置**

采用标准 1U 机架式设备；交流冗余电源；具备 12 个千兆电口，12 个千兆光口；最大并发连接数为 200 万；每秒新建 TCP 连接数为 5 万条；网络吞吐量为 8Gbps；应用性能不小于 4Gbps；

- **功能描述**

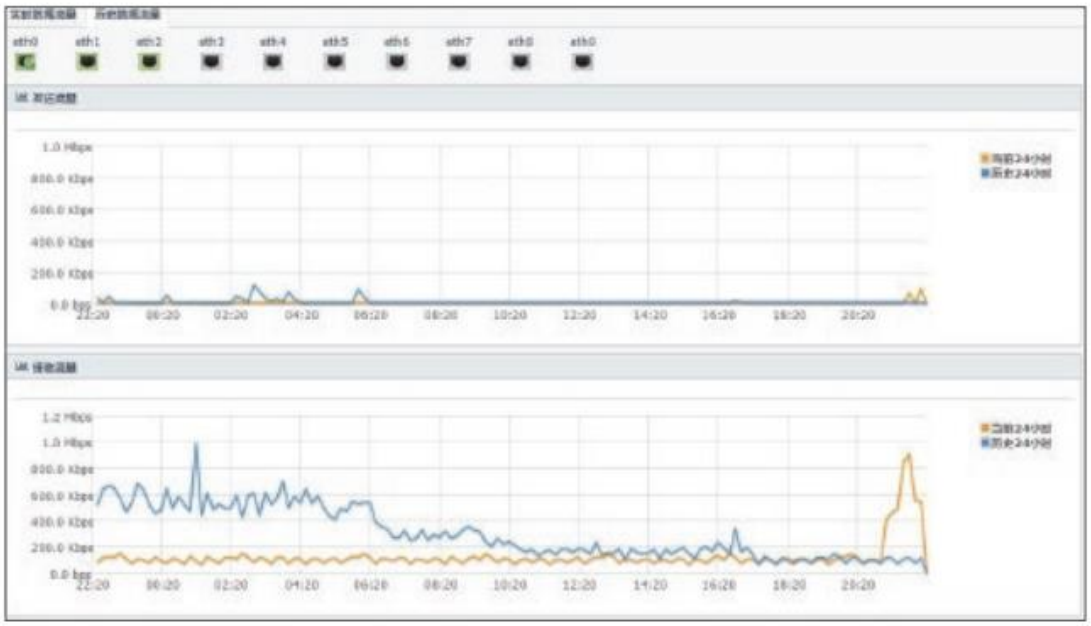
链路负载均衡

东软 NetEye 入侵检测支持链接负载均衡，通过基于接口、域名进行链路负载均衡，负载均衡接口只是 pppoe、dhcp、tunnel、物理接口等三层接口，负载均衡算法包括优先级和权重。

全面的入侵检测，抵御恶意网络流量

检测引擎提供了从网络层到应用层全面的攻击防御功能。针对当前主要的应用层攻击，能够深入到应用的内容层进行检查，及时发现 XSS、SQL 注入 等常见应用层攻击并有效阻断。同时，还能够针对底层有效过滤 IP/端口扫描类攻击、

DoS/DDoS 等异常流量型攻击。东软 NetEye 入侵检测拥有完善的特征库，特征库数量大于 21000+；100+工业协议应用识别，可实时展示应用流速和统计信息；



内容恢复

系统可对常用应用协议（如 HTTP、FTP、SMTP、POP3、TELNET、IMAP、DNS 等）提供内容恢复功能，能够完全记录通信过程与内容并将其按照 应用界面风格进行直观展现。此功能对于分析攻击过程、监控内部网络资源滥用、发现未知攻击等需求极具价值。

多重报警响应方式及实时提醒

系统支持实时报警、记录到数据库、电子邮件报警、SysLog 报警、SNMP Trap 报警、切断攻击连接等多种报警方式，便于及时通告并触发后续处置流程。

实时安全防护，漏洞修复无时差

作为 CVE 兼容认证成员，检测引擎拥有规范、全面的漏洞规则库，保障规则匹配效率。同时，作为微软“MAPP”（Microsoft Active Protections Program）成员，检测引擎能够在微软对外公布安全漏洞信息之前提前获取漏洞细节信息，及时更新特征库和升级补丁，第一时间为客户提供安全保护。