入侵检测系统

精准攻击识别，旁路分析审计

**产品概述**

捷普入侵检测系统采用了新一代的多样性智能检测方法、规则关联分析和数据挖掘技术，能够实时检测包括溢出攻击、RPC攻击、WEBCGI攻击、拒绝服务攻击、木马、蠕虫、系统漏洞等各种网络攻击行为，并可分析发现潜在的未知APT攻击以及违反企业安全策略的P2P下载、IM即时通讯、网络游戏等资源滥用行为，通过多样化告警方式，及时向管理员发送预警信息，能够与防火墙等网关防护产品形成纵深防御体系为用户提供完整的立体式网络安全检测监控服务。



* **易部署：**配置简单方便，B/S管理模式，可做到用户零配置，支持分布部署，无需特殊部署方案。以旁路接入网络，不会影响到业务数据的正常通讯。
* **易使用：**图形方式显示入侵事件的发生及对入侵事件的详细描述，使非专业人员更容易理解和操作；通过重点检测用户常用应用，避免海量报警的爆发。
* **更专业：**具有专业的分析和评估能力；使用不同分析手段的图形化表示方法，彻底变革传统IDS单一报警方式；采用数据挖掘技术，将趋势和报警结合起来，达到了预见性报警和事后分析的完美结合。
* **更合规：**通过深入的二到七层的双向检测，合规性满足用户对等级保护、分级保护以及相关行业法规的要求。

**产品特点**



* **高效的数据包采集**

采用捷普独有的多核处理硬件平台，基于网络流量全镜像的数据包采集和零拷贝技术，实现网络数据包的无损复制和采集，并可深入到应用层，增加了系统的安全和处理控制能力，具有极高的性能。

* **高检出率的保证**

5000+条检测规则，从危险程度、攻击手段和服务类型三个角度划分为多种规则对象；全面覆盖Windows、Linux、Solaris、ALX、BSD等操作系统，实现了对攻击行为的全面识别和检测，以及对流行病毒木马、APT的检测；规则库经国际权威组织CVE以及国家漏洞库CNNVD的兼容性认证，专业的攻防安全团队作为技术支撑，保持规则库至少每周一次的更新频率。

* **独特的未知攻击发现技术**

系统应用了独特的网络未知异常安全监测和关联挖掘分析技术，可以更加精确地掌握网络实际运行状态，为判断未知攻击提供了有力的依据；并能够有效识别各类攻击规避技术，为用户提供全面的安全检测能力。

* **直观可视的分析评估**

系统提供了分析评估中心，可以将网络中的数据详细分类，对入侵报警和流量进行全面分析，应用全图形化分析手段，直观可视的展现收到网络威胁的全部信息。网络管理员可以根据当前网络安全对比情况，进行合理的调整；结合基于资产的识别，在分析评估的基础上快速、准确定位攻击及违规行为责任人。

* **智能化的自动阻断**

系统提供两种方式进行阻断，一种是通过发送RST包或不可达包实现，另一种是与防火墙、IPS进行联动，由防火墙完成阻断功能；系统采用智能控制阻断方法，可以对最具威胁IP进行集中阻断，并且每条系统规则都给出了缺省的最佳响应方式。

* **IPv4/IPv6双协议栈支持**

完善支持IPv6通讯流量，为IPv6网络提供安全解决方案，零投入实现安全防护能力的下一代迁移。

* **独有的全网安全预警解决方案**

在充分考虑网络检测全方位、全面性的设计理念，通过深入内网的软件探针攻击检测技术，实时侦测网络中任何可疑行为，并提供全局性的安全预警。

* **全面的入侵检测状态评估和分析**

可对网络中入侵报警，对流量进行全局分析和评估，可对不同的主机或者网段进行单独分析和评估，挖掘查询系统，为用户提供实时、可视的安全状况查询。

**产品功能**

入侵检测
采用了先进的基于目标系统的流重组检测引擎，从根源上彻底阻断了TCP流分段重叠攻击行为。智能资产关联，将检测事件与资产实际情况结合，提高检测准确度。逻辑关联，将事件进行归并处理，可有效解决海量日志问题。拥有5000+条攻击规则，有效的保证了检出率。
DoS/DDoS检测
全面支持DoS/DDoS防御，可防御SYN flood、ICMP flood、UDP flood、Winnuke、TcpScan以及CC攻击，支持DNS、SNMP、NTP等协议的放大攻击的检测。提供异常流量自学习功能，根据用户实际业务情况推荐DoS/DDoS检测策略。通过和其它防护类设备进行联动，实现DoS/DDoS攻击的防御。
应用检测
能够识别包括传统协议、P2P下载、股票交易、即时通讯、流媒体、网络游戏、网络视频等在内的超过1200种网络应用，使用户很轻松判断网络中的各种带宽滥用行为，通过和其它防护类设备联动实现阻断、限制连接数、限制流量等，确保网络业务通畅。
病毒检测
采用基于数据流的检测技术，能够检测包括木马、后门和蠕虫在内的各类种网络病毒。与传统的防病毒网关不同，不需要依据透明代理还原文件，而是直接在数据流中检测病毒，实现高速在线检测，实时阻断新近流行危害度最大的各种网络病毒。
URL检测
内置庞大的URL分类库，库中收纳包括恶意网站、违反国家法规与政策的网站、潜在不安全的网站、浪费带宽网站、大众兴趣的网站、聊天与论坛网站、行业分类网站和计算机技术相关网站等。能够统计分析内网用户的上网行为，检测对恶意网站或者潜在不安全站点的访问。通过与和其它防护类设备联动，可以制定有效的管理策略，实现内网用户的上网行为管理。 无线攻击检测
提供无线网络边界入侵防御功能。针对引起无线信息安全的Ad-hoc、私接AP、非法外连、无线钓鱼、无线代理等无线攻击做到有效防护，可同时提供有线网络边界、无线网络边界的攻击防御。

|  |  |
| --- | --- |
|  | **典型部署** |

针对结构越来越复杂的网络环境，捷普入侵检测系统提供全面而深入的检测解决方案，通过分布式和软件子探针的灵活部署方式，在网络核心区、DMZ区、办公区内部、分支机构接入区等关键节点部署入侵检测系统，并通过捷普入侵检测系统集中管控，实时掌控全网安全状况。

