聚铭入侵防御系统

产品白皮书

聚铭网络科技有限公司

2024 年 04 月

目录

声明

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

北京总部：北京市海淀区丹棱街 18 号创富大厦 9 层

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

1. 前言

随着网络与信息技术的发展，尤其是互联网的广泛普及和应用，网络正逐步改变着人类的生活和工作方式。近年来，移动互联网、社交网络和云计算的兴起，促进了互联网的发展。伴随着网络的发展，也产生了各种各样的安全问题，网络中蠕虫、病毒及垃圾邮件肆意泛滥，木马无孔不入，DDoS 攻击越来越常见，黑客攻击行为几乎每时每刻都在发生。如何及时的、准确的发现违反安全策略的事件，并及时处理，是广大企业用户迫切需要解决的问题。

聚铭入侵防御系统（Intrusion Prevention System）作为防火墙的补充，入侵防御系统被认为是防火墙之后的第二道安全闸门，对网络进行检测，提供对内部攻击、外部攻击和误操作的实时监控，并提供动态保护，大大提高了网络的安全性。 入侵防御系统能够在入侵攻击对网络系统造成危害前，及时检测到入侵攻击的发生，并进行报警，被入侵攻击后，入侵防御系统可以提供详细的攻击信息，便于取证分析。

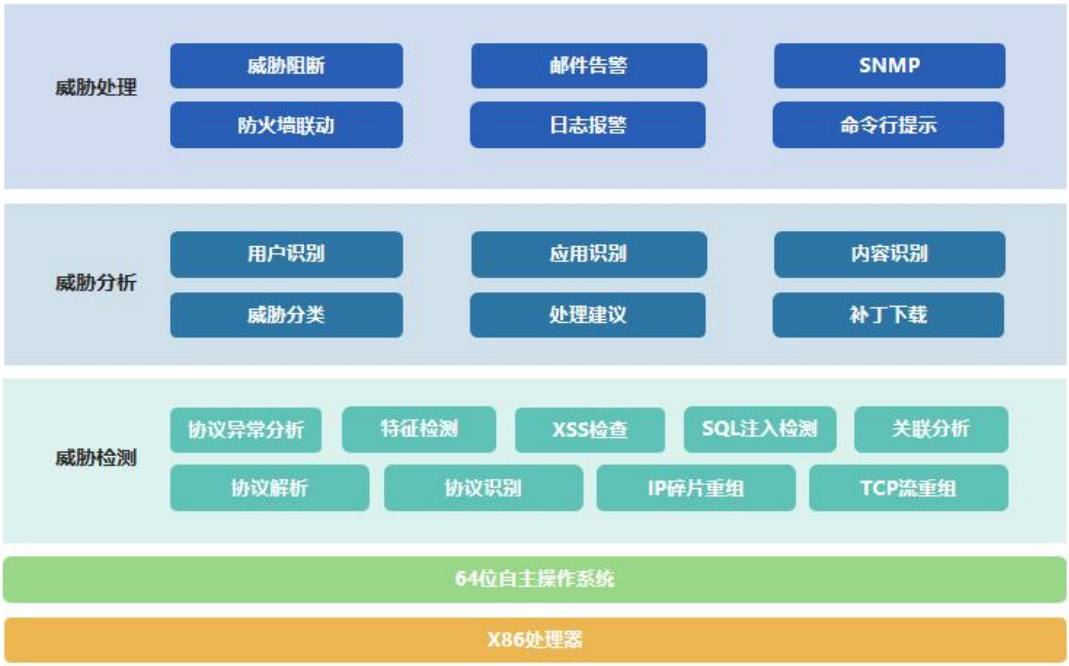
聚铭入侵防御系统提供动态防御能力，在网络部署中有效结合防火墙和入侵防御系统，能够给网络带来全面的防御。入侵防御系统很好的弥补了防火墙的不足，通过部署入侵防御系统，可以有效的监视网络中的所有实时传输数据，提供专业全面入侵检测能力，通过协议状态检查和智能关联分析，提供给用户全面的信息展现和安全预警，为改善用户网络的风险控制环境提供决策依据，是整个网络体系中不可或缺的一部分。

2. 产品介绍

聚铭入侵防御系统对缓冲区溢出、SQL 注入、暴力猜测、DoS 攻击、扫描探测、蠕虫病毒、木马后门等各类黑客攻击和恶意流量进行实时检测及报警，并通过与防火墙联动、发送邮件、SNMP trap 等方式进行威胁防御。

2.1. 产品架构

聚铭入侵防御系统基于多核硬件平台，使用基于多年技术积累自主研发的操作系统，当前系统由威胁检测、威胁分析、威胁处理三大部分组成。



2.2. 硬件架构体系

聚铭入侵防御系统采用多核并行处理架构，其最大的特点是拥有强大的计算能力和应用处理能力，足以应付入侵防御系统需要的计算需求。

2.3. 软件架构体系

聚铭入侵防御系统是基于聚铭自主研发的专用网络操作系统，作为新一代的模块化操作系统，拥有良好的稳定性、安全性，具有广泛的新特性支持，构成了产品新的核心竞争力。

聚铭入侵防御系统通过采用聚铭自研的安全平台，使聚铭入侵防御系统拥有更加广泛的适用性，能够有效推动操作系统更快速地升级和优化，对系统的功能丰富性和系统稳定性都有帮助。安全平台可灵活扩展软件功能，为满足现在及未来各种用户应用需求打下坚实的基础。

2.4. 合规性要求

根据《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）等级划分原则，聚铭入侵防御系统满足第三级以内的要求，具体内容如下：

等保等级	对应项	具体内容
第三级	8.1.3.3 入侵防范	a） 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； b） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； c） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
	8.1.3.4 恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

3. 产品特点

3.1. 基于流重组高效检测

现有的入侵防御产品中，绝大部分产品属于单包过滤产品，他们的特点是拥有高性能的处理，却牺牲了攻击检测阻断的准确性。而当前流行的网络攻击方式

和种类是逐步向网络上层延伸的，攻击行为常常隐藏在 7 层应用的数据流中，大量的攻击数据流都是封装在标准的应用协议数据流中，通过通用的端口进行伪装，欺骗无法进行流重组和协议分析的入侵防御产品。而基于单个数据包检测的入侵防御产品更是无法有效抵御 TCP 流分段重叠的攻击，很多的攻击行为通过 TCP 流分段组合即可轻松穿透这种引擎，使受保护的目标服务器上形成真正的攻击。在攻击检测的过程中,为了准确有效的检测出隐蔽在多个数据包中的攻击,必须进行 TCP 会话的还原,从而得到完整的攻击特征。

3.2. 基于协议状态分析

聚铭入侵防御系统的协议分析技术，是对已知协议和 RFC 规范的深入理解，可准确、高效的识别各种已知攻击。同时根据系统协议分析的算法，协议分析引擎拥有检测协议异常、协议误用的能力，彻底解决了以往基于模式匹配技术的入侵防御产品片面依赖攻击特征签名数量来检测攻击的弊端，极大的提高了检测的效率，扩大了检测的范围。聚铭入侵防御系统目前支持 Telnet、FTP、HTTP、SMTP、SNMP、DNS 等多达 30 种的主流应用层协议，遥遥领先于其他入侵防御系统品牌。

目前聚铭入侵防御系统所采用的基于协议状态的检测技术，使它具有了明显的优势：

- 利用协议分析，在处理数据帧和连接时更加迅速和有效准确，减少了误报的可能性。
- 能够关联数据包前后的内容，对孤立的数据包不进行检测，这和普通入侵防御系统检测所有数据包有着本质的区别。一方面因为这种检测机制的高效性降低了系统在网络探测中的资源开销，大幅度提高了检测性能，另一方面因为在攻击指令到达操作系统之前，模拟了它的执行，以确定它是否具有恶意，有效减少了误报。
- 它具有判别通信行为真实意图的能力，它不会受到像 URL 编码、干扰信息、IP 分片等入侵防御系统规避技术的影响。

当检测到的所有数据信息经过应用协议分析后， 聚铭入侵防御系统将真实的应用数据与签名库进行攻击特征的匹配，因为我们知道特征匹配仍然是检测效率最高的和最准确的检测技术。只是这种匹配，与普通基于模式匹配的检测机制有着本质上的区别，它是在协议分析和还原以后真实有效的数据，这种真实可靠的有效数据的匹配，一方面提高了检测效率，另一方面，增强了检测攻击的准确度，减少了误报的概率。

3.3. 智能关联分析

由于聚铭入侵防御系统可以监听网络内部的通讯，无论是内部主机直接的威胁还是从外到内的威胁，都可以及时报警，从而提醒网络管理员来处理存在的威胁。在大规模蠕虫爆发时，聚铭入侵防御系统的预警，使得管理员能及时采取行动，从而极大地避免了网络崩溃导致的危害。

聚铭入侵防御系统作为对网络攻击检测的产品，全面检测能力是其重要指标。而特征库是入侵防御系统的检测核心部分，因而很多时候检测的全面性被简化为特征库的数量，出现在招标要求或者产品的指标中。而另一个方面，同一个网络数据包，在有的网络环境下是威胁，而在有的网络环境下则是完全正常的行为，这样就只有将这样的行为都定义在默认的特征库中，因此通常情况下特征库中会出现“Ping”、“HTTP 连接”甚至“TCP 连接”这样的事件。

当前各种入侵防御产品产生的报警，往往都需要经过人工分析，才能筛选掉出重点关注事件。分析步骤一般如下：

- 对事件本身的性质进行判断。大多数入侵防御产品都能对 ping、tcp 连接等事件进行报警，一般情况下安全级别较低的报警不需要关注，如果有大量报警产生的话，确认一下是否是正常业务产生即可。
- 通过结合网络环境来判断。首先需要确定攻击对象和攻击者的性质、在网络中的位置。比如 SNMP 查询这样的事件，需要确认源地址是否正常的网管软件，如果就是合法的网管软件在工作，这样的事件就不

需要继续关注了，如果不是则需要确认是错误地配置了网管软件还是被控制来扫描了。而对于攻击对象需要确认漏洞是否真实存在。

- 这个攻击是否流行。如果攻击针对的漏洞是几年前出现的，这样攻击的威胁成功率就比较低。
- 是否是特定关注，比如有些网络中不允许出现网络共享，因此如果出现针对网络共享的攻击必定需要仔细核实。

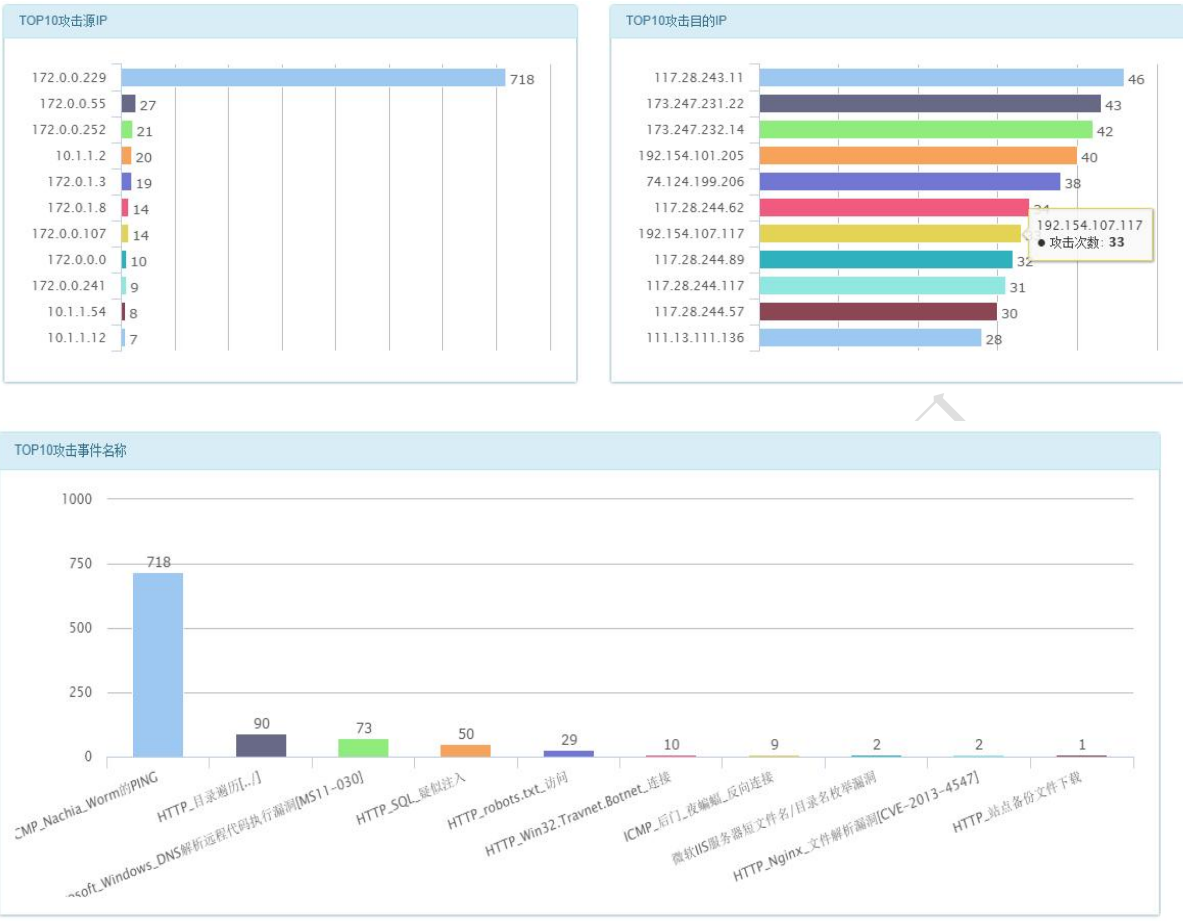
从以上步骤可以看出人工分析事件的时候，需要结合多个维度的信息进行分析。结合其多年产品研发经验和对大量客户使用过程的研究，将实现对报警的智能分析系统，抑制海量事件，突出展现重点关注事件，必将推动行业向智能化方法发展。

3.4. 专业的病毒防护

聚铭入侵防御系统拥有海量病毒特征库，配合高速防病毒引擎，能够精准识别并阻断流行木马和顽固病毒入侵。查杀范围包括病毒、木马、蠕虫、后门、间谍软件、恶意程序以及 HTTP\FTP\SMTP\POP3\IMAP 等主流应用协议，数百万病毒特征全库，特征库定时在线更新。针对纯扫描优化的产品架构，无系统监控，不占系统资源，是保护内网资源不受互联网病毒侵扰的最佳选择。

3.5. 全面的日志审计

聚铭入侵防御系统全面审计各种网络入侵行为，并对网络入侵日志进行多维度的统计和分析，以柱状图等丰富的图表形式进行展示，使得管理员能够一目了然的获知全网的网络入侵和攻击趋势，以便于及时响应。



3.6. 灵活的安全策略管理

聚铭入侵防御系统采用基于策略的防护方式，内置了多种默认安全策略集，用户可以根据需要选择最适合当前使用场景的策略，以达到最佳防护效果。 用户可以根据防护的类型不同而选择不同的事件集，既可以提高系统的性能，也可以减少误报的发生机率。

聚铭入侵防御系统，可以根据安全类型、协议类型、系统、级别、事件来源等多个方面来灵活的选择安全策略。同时对于不同的安全策略，可以自定义不同的防护级别，适用于各种不同的场景。

4. 部署模式

4.1. Inline 工作模式

聚铭入侵防御设备通常部署为 Inline 的工作模式，能够识别、阻断公司或运

营商的外网对内网用户的攻击行为，及时阻止各种针对系统漏洞的攻击，屏蔽蠕虫和间谍软件等。

在数据传输的路径中，任何数据流都必须经过聚铭入侵防御系统设备做检测，一旦发现有蠕虫、后门、木马、间谍软件、可疑代码、网络钓鱼等攻击行为，聚铭入侵防御系统模块会立即阻断攻击，隔离攻击源，屏蔽蠕虫和间谍软件等，同时记录日志告知网络管理员。

4.2. Passive 工作模式

在此工作模式中，相当于 IDS 设备，网络的流量不会流经聚铭入侵防御系统，而是由其它网络设备把需要检测的流量镜像一份给入侵防御系统。在这种部署模式下，聚铭入侵防御系统设备不会影响网络的正常运行，也可以通过与防火墙联动等手段来阻断攻击。