聚铭入侵防御系统产品白皮书

聚铭网络科技有限公司

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

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

1 需求概述

随着互联网的飞速发展，网络的资源共享进一步加强，网络形势正发生着日新月异的演变，层出不穷的新型威胁冲击着现有的安全防护体系。传统的安全和产品体系使用单机的、私有的思路来解决网络的、公有的已知威胁。面对未知的安全威胁需要采取综合的、全方位的防御策略，并保持敏锐的警觉性。基于协同防御体系的新一代网络安全防御系统以分析中心、数据中心和处置中心为核心，旨在为政府、军队、金融、教育、运营商和企业的网络出口提供集威胁分析、定位和处置为一体化的功能。它旨在提供对威胁进行全面分析、确定位置和采取应对措施的能力。

防火墙作为企业级安全保障体系的第一道防线，已经得到了非常广泛的应用，但是各式各样的攻击行为还是被不断的发现和报道，这就意味着有防火墙不是万能的。防火墙等访问控制设备没有能做到完全的协议分析，仅能实现较为低层的入侵检测，对应用层攻击等行为无法进行判断。

入侵检测系统（Intrusion Detection System）是对防火墙有益的补充，入侵检测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，提供动态保护大大提高了网络的安全性。

2 产品特色

2.1 深度安全检测

聚铭入侵防御系统具有数据深度安全检测能力和攻击防御能力。主要包括：

可支持DoS/DDos防护、畸形IP报文、异常TCP报文，也可支持系统漏洞防护、间谍软件防护、木马、注入攻击、Web应用攻击、病毒等检测和防护。并且对内容过滤、文件过滤、URL过滤和网络行为管理是常用于网络管控的功能，以确保网络安全和合规性。

威胁情报要基于海量数据才能生产出来支持强大的威胁情报，通过本地威胁情报检测功能快速对用户网络中的未知威胁进行检测和识别。

2.2 强大的识别功能

采用DPI/DFI融合识别技术，能够进行全面和深入识别应用，可支持9000+种以上的应用协议，也可手动自定义特定应用，支持深度内容检查技术。

基于状态机的多模匹配算法，对待匹配的数据形成了一个高效的匹配矩阵，可发现所有出现的关键字。过滤时间与数据长度成正比，和设定的关键字数目无关，算法分析复杂

度是O(M+N)，N是数据长度，M是关键字数量。可见此算法对数据长度与及并键字数量具有线性复杂度，比起传统的单模匹配算法大大提高了效率。

支持对蠕虫、病毒、木马、僵尸网络、间谍软件、广告软件、CGI攻击、跨站脚本攻击、注入攻击、目录遍历、信息泄露、远程文件包含攻击、溢出攻击、代码执行、拒绝服务、扫描工具、后门等类型攻击的检测和防护；

2.3 应用及流量可视化

聚铭入侵防御系统为用户提供了全面的、实时的风险信息展示，着重突出应用类型分布、威胁事件、攻击趋势图，一键直达异常行为跟踪界面。配置威胁分析模块和流量分析，可通过自定义关键字模糊检索，定位异常行为踪迹，加之对漏洞、应用、会话、网络的全方位监控与分析，确认异常行为和风险。

2.4 带宽优化管理

基于深度DPI识别技术对网络流量的内容进行分析和识别，可以判断流量所承载的应用服务，支持10000+应用服务、自定义服务和自定义特征的管理。可提供最大带宽、保证带宽和预留带宽等多种带宽管理手段，并提供基于用户、应用、时间、网络接口等多种组合条件的带宽管理策略，满足管理员对用户及应用带宽管理策略的灵活性要求。

基于应用识别的P2P抑制技术，在大流量情况下判断是否为P2P应用并进行抑制，减少此类应用对网络资源的占用，保障其他业务的正常运行。

策略优先级保障系统可对网络流量进行分类和标记，为重要业务提供优先传输保障，确保其稳定运行。

2.5 丰富的身份认证

本地认证：Web认证、用户名/密码认证、IP/MAC/IP-MAC绑定；

第三方认证： LDAP、RADIUS、POP3、数据库、Oauth、CAS等；

短信认证：通过接收短信获取验证码，快速认证；

社交账号认证：微信认证，飞书认证，钉钉认证；

访客二维码认证：授权扫描访客手机上的二维码，备注信息后，访客即可通过认证，支持多场景使用；

双因素认证：USB-Key、指纹认证；

单点登录：AD域、PPPOE、Radius、WEB和第三方系统等读取认证账号；

按照组织的行政结构建立树形用户分组，实现父组、子组等多层嵌套的要求，同时满足不同用户和用户组网络访问权限控制。

2.6 全面、智能的路由功能

聚铭入侵防御系统支持全面、完善的路由功能。支持静态路由、策略路由、ISP路由，RIP、OSPF、OSPFv3、BGP等路由功能。并提供更广泛的IPv6网络支持。这样可以增强网络安全性并确保系统在现代化网络环境中的兼容性。在多出口的环境中根据用户实际需求，匹配多种方式的负载均衡算法，包括备份、源目地址轮询、源地址轮询、最优链路、上行流量负载、下行流量负载等。可以实现基于权重的路由负载、基于延迟的路由负载、基于会话的路由负载、基于流量的路由负载，满足用户各种场景。

3 技术实现

聚铭入侵防御系统以识别上网应用，创新技术手段，有效管理网络，多层面自身安全防护，多种灵活部署方案，直观丰富的分析报表等产品特点设计。对于网络资源的滥用，封堵还是放任，这是摆在网络管理者面前的难题，聚铭入侵防御系统产品提供了灵活的管理策略，根据企业的需求，定制个性化的管理方案，帮助各企业建立安全、高效、健康、和谐的网络环境。

3.1 安全特性

在完全继承和发展传统安全功能的基础上，提供完整丰富的应用识别和应用层威胁、攻击的防护能力。

3.1.1 安全策略

聚铭入侵防御系统的安全策略是聚铭入侵防御系统的核心功能，是聚铭入侵防御系统实现访问控制的基础。

聚铭入侵防御系统支持基于状态检测和应用层数据识别的动态包过滤技术。通过源安全域、目的安全域、源IP地址、目的IP地址、用户、服务、应用、时间等维度对数据进行识别，将用户需要进行过滤及控制的数据流分离，并实现精细管控。

同时，聚铭入侵防御系统支持对相应的数据实现反病毒、漏洞防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控的一体化策略配置。

3.1.2 IPS引擎

采用全新先进的多维动态特征异常检测引擎，抛弃原有的异常行为特征码静态表达的方式，将异常行为、漏洞特征通过多维度提炼，动态进行表达，使得特征表达更加全面、精准、有效，极大提高了聚铭入侵防御系统聚铭入侵防御系统的命中质量，解决了传统设备检测命中率高，但是误报率同样高的问题。

3.1.3 病毒防护

内置海量病毒特征，配合先进的防病毒引擎，能够精准识别并清除流行木马和顽固病毒。病毒检测引擎针对非缓存流检测模式进行了全面结构调整和优化，使下一代聚铭入侵防御系统的病毒检测率和处理性能获得质的突破。

- 协议包括：FTP、HTTP、SMTP、POP3、IMAP。
- 支持路由、透明、混合等各种工作模式下的网络病毒检测
- 采用高效的病毒防御引擎和国内知名病毒厂商特征库，可检测不少于400万以上种病毒。
- 支持对压缩文件进行扫描和过滤，最大解压层数为16层。

3.1.4 状态检测

内置基于状态检测技术的会话，支持高并发状态检测，对进出内网的数据包进行控制。内网用户可以通过NAT规则转换IP地址上网，NAT功能主要分为内网代理、一对一地址转换以及端口映射，能够更有效的保护内网上网安全，而对于非法报文，不符合会话检测状态的报文果断拒绝，有效地保证内外网有效带宽的有效利用。能够识别并阻断黑客的端口扫描以及普通的DoS攻击行为，保证内部网络的安全性。同时，系统也阻断了内网的垃圾数据包对聚铭入侵防御系统资源的消耗，大大降低了聚铭入侵防御系统工作的负担，提高了整体网络的安全性。

3.1.5 Web防护

Web防护引擎，可以有效抵御各种注入式攻击，包括SQL注入、系统命令注入、LDAP注入、SSI注入、邮件注入、请求体PHP注入等攻击。对于常见的XSS攻击的防护结合基于语义分析和攻击指纹两种方式，相比传统只基于攻击指纹的检测方法，检测准确率更高，误报率更低，防逃避能力更强。

3.1.6 威胁情报

整合对接多来源威胁情报，支持对可疑IP、域名进行搜索，并查看关联分析，支持与威胁情报云平台对接，用威胁情报发现内网有威胁的会话，支持对内网产生的威胁进行分类，管理员可以根据实际情况，对内网威胁进行处理。

3.1.7 攻击防护能力

聚铭入侵防御系统基于安全域，支持多种类型的攻击防护。

Flood防护包括SYN Flood、ICMP Flood、UDP Flood、IP Flood、SIP Flood和HTTP Flood防护等。

恶意扫描防护，包括IP地址扫描和端口扫描。

异常包防护。包括ping of death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke和IP分片等。

IP异常报文包括错误的IP报文选项防护、IP时间戳选项报文防护、IP安全选项报文防护、IP数据流项报文防护、IP记录路由选项报文防护、IP宽松源路由选项报文防护、IP严格源路由选项报文防护。

TCP 异常报文SYN数据分片传输防护、TCP报头标志位全为0防护、TCP报头标志位全为1防护、PSH,FIN和URG标志位同时为1防护、SYN和FIN标志位同时为1防护等

3.1.8 应用访问控制

门户网站、社区论坛、交友网站、博客、个人网页，网络上五花八门、包罗万象的网页吸引着网民的眼球，诱惑网民拿起鼠标去体验网络的乐趣。在企业里，很多员工利用上班时间泡论坛、炒股、玩游戏、收发私人邮件、聊天等等，影响了工作氛围，降低了工作效率，浪费了企业资源，这是所有企业管理者都不希望发生的。

为避免企业为员工的这些不良行为买单，提供了细致的上网行为管理方案，对用户的上网行为进行细致而灵活的管理，进而提高员工的工作效率，避免机密信息的泄漏。

- URL过滤：内置了数百万的 URL 资料，分为新闻、音乐、视频、广告、财经、教育、科学、房地产、求职招聘等URL组；
- 搜索引擎关键字过滤：记录用户通过搜索引擎类网站搜索的关键字内容，并基于搜索类别、关键字内容，过滤用户的非法搜索行为；
- 发帖关键字过滤：对发帖的内容启用关键词过滤，对含有攻击领导人、分裂言论、下流词汇，或者伤害公司利益的帖子进行审计和过滤处理，并能对所有成功上传的内容进行详细记录以便事后查验；
- 文件传输过滤：针对不同的文件类型，对IE/FTP的上传或下载进行跟踪、阻断或者限速。帮助企事业单位防止员工泄密，净化网络流量，提高内网的安全性；
- 邮件过滤：对SMTP、POP3、WebMail等进行审计，能够对用户收发邮件的时间、标题、内容以及附件等等元素进行过滤和完整的内容记录，避免企业、机关敏感信息泄露。

3.2 系统管理

3.2.1 管理员认证

聚铭入侵防御系统支持以HTTP及SSL加密的WEB图形化接口进行设备配置和管理，对于多次登录失败的用户，会弹出额外随机文字图形进行验证，还会对来源IP进行锁定，限制登录，避免遭受暴力破解攻击。同时支持定期提醒或强制管理员周期性修改密码，避免密码外泄带来威胁，支持密码强度、密码使用时长、口令尝试死锁、账户激活等安全管理功能。

支持SSH和telnet进行维护管理，忘记密码支持Console管理登录恢复初始密码，支持网管策略，缺省关闭外网网管，还可允许部分IP能网管设备，以限制非法管理员访问设备。

3.2.2 权限管理

聚铭入侵防御系统管理权限分立：系统默认有超级管理员、审计管理员、只读管理员，可根据需要灵活定制管理员角色。定制的管理员可限制页面访问的目录树，对金融类审计安全要求的场景，支持审计管理员Dkey绑定，离开Dkey将无法查看审计日志。

3.2.3 登录页随机编码

为了防止黑客攻击，特别是爬虫扫描登录页获取设备指纹，聚铭入侵防御系统对首页进行周期随机编码重写，登录首页编码文本内容经常变化，单纯地根据首页特征，黑客无法判别聚铭入侵防御系统或者版本，防止资产扫描或爬虫获取有效的特征信息，而从无法针对性发出定向攻击。

3.2.4 多语言支持

聚铭入侵防御系统的Web管理界面支持中英文，登录时设备根据浏览器语言选择相应的语言，管理员也可在首页上选择语言登录。

3.3 应用识别

应用识别（Application identify)是下一代聚铭入侵防御系统的重要功能。借助于应用识别功能，可以准确识别网络上正在运行的应用，应用流量的准确识别不但可洞悉整个网络的运行情况，而且可针对具体需求做用户行为的准确管控，这在一定程度上既可保证业务流的高效运行也可预防由于内网机器受到攻击而生产的威胁，同时识别应用类型也是应用审计与应用流量控制的基础。

3.3.1 应用识别

聚铭入侵防御系统支持应用识别库，内置9000+应用特征。通过应用识别库，聚铭入侵防御系统可以对流量进行应用识别。

基于应用的流量识别和管控，用于限制网络内部的用户使用某种指定的应用程序，能够差别化地限制某些影响工作效率或占用大量带宽应用的使用。

3.3.2 服务识别

聚铭入侵防御系统支持基于TCP、UDP协议和网络层协议，通过源端口号、目的端口号以及协议号进行服务识别。

聚铭入侵防御系统内置有常用协议的服务库，用户在使用时可以直接选择库中的协议。还支持自定义服务，通过TCP、UDP协议的源端口号和目的端口号来定义服务。

内置的服务和自定义的服务可以作为安全策略的一个属性，实现基于服务的精细化流量管控。

3.3.3 自定义应用

办公自动化的趋势下，客户内网均已搭建了企业的应用系统，例如OA、ERP系统等。面对这种情况，上网行为管理产品通过自带的应用特性库无法对企业应用系统机型识别、审计和管理。下一代聚铭入侵防御系统具备自定义应用功能，管理员可根据协议、目标端口、IP、域名等维度创建应用特征，进而针对企业应用进行审计、流量统计和控制。

3.3.4 内容识别

基于深度内容识别的行为管控策略，内容识别功能即支持文件内容识别，也支持应用内容识别。用于限制企业内部网络机密信息的传播，从而降低公司机密泄露的风险，保证信息安全。

3.3.5 URL识别

支持基于URL的识别和管控，内置千万级预分类URL地址库，也支持自定义URL。基于URL的识别和管控，用于限制企业内部网络用户访问某些恶意的URL。例如禁止访问恶意URL、暴力反动、挖矿的URL等。

3.3.6 SSL流量内容识别

SSL内容识别：SSL审计技术可对HTTPS加密网站的审计，包含发帖行为、网页浏览行为、SSL加密邮件等加密应用进行内容级审计。

3.4 黑白名单

3.4.1 黑名单

将IP、域名加入到黑名单中，并支持黑名单时长设定，网络中的流量触发防攻击规则后，自动将源地址加入黑名单中，有效提升了用户网络安全性。管理员可以手动添加黑名单拒绝某些非法的 IP 地址或域名地址的流量，分为永久封锁和生命封锁。IP地址支持IPv4和IPv6地址。

3.4.2 白名单管理

白名单功能包括IP地址白名单、URL白名单、即时通讯白名单。IP地址白名单和URL白名单表示：对内网中某些用户访问的IP地址或URL地址不做控制和记录。即时通讯白名单表示：对即时通讯软件的某些账户不做控制和记录。

3.5 用户管理

用户是聚铭入侵防御系统产品的基本要素，任何的行为管理策略都是以用户为核心。因此，对于用户的识别、认证与管理成了行为管理的前提要素，同时也决定了行为管理的效果。聚铭入侵防御系统产品通过不断地深入实践与研发，提供了灵活的用户管理方式，很好的满足了广大企业对用户管理的需求。

3.5.1 组织结构

对于用户数比较多的企业，有清晰的组织结构非常重要，便于管理员对用户的管理、查询和定位。聚铭入侵防御系统通过多叉树特殊的数据结构，用户和用户组都只是这颗多叉树上的结点，支持树型结构的用户管理，并且不同的用户组之间可以灵活的调整成员用户，从而可建立与企业行政组织结构相同的网络组织结构，如下图所示：

3.5.2 自动分组

对于用户数比较多的网络环境，第一次构建组织结构时，如果让管理员手动的去建立每一个组和用户是很不现实的。在大多数情况下，管理员并不会对每一个用户单独的设定一个管理策略，而是针对某一类用户进行统一的管理。所以自动的创建用户组和自动的分配用户就显得非常重要。

聚铭入侵防御系统支持将新入网还未在组织结构中的用户，根据预设的IP网段和策略配置表进行自动分组并设定策略。新入网的用户可以根据其IP地址、MAC地址、主机名、VLAN ID等多种方式来定义用户名，可以达到各种网络环境的需求，如静态IP环境、DHCP环境等等。每个用户还支持别名的功能，管理员可以为其添加别名，以更加直观的方式来呈现用户，为后续的行为审计、统计奠定了基础。

对于外来访问的临时用户，管理员可以为其分配一个特定网段，将其加入临时用户组，并预设一定的访问权限。同时可以设定用户离线多久就自动删除该用户，从而大大的简化了动态用户的管理，增强了用户管理的灵活性。

3.5.3 内网主机扫描

聚铭入侵防御系统可通过NetBIOS协议扫描内网的主机信息，扫描结果将列出每个主机的IP地址、MAC地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理。另外，在对用户进行IP/MAC绑定时，管理员只需要输入某个主机的IP或者MAC等信息，就可以扫描出对应的其它信息，从而大大简化了管理员的工作。

3.5.4 用户导入

除了自动分组和内网主机扫描以外，聚铭入侵防御系统还支持批量导入用户的方式，以多种灵活的方式方便管理员建立组织结构：

- 自定义文件：可将管理员定义的包含批量用户的Excel文件导入系统，从而批量建立用户组和用户。
- LDAP/AD用户导入：可将LDAP/AD服务器中的用户信息导入组织结构中，并自动创建默认的组权限，同时，聚铭入侵防御系统还支持定期与LDAP/AD服务器同步用户信息，实现用户的定期更新。从而实现了与原有网络管理平台的结合，达到了全网用户统一管理的目的。

3.5.5 多种身份认证方式

身份认证都是通过认证策略表匹配来实现的，用户身份认证有两种方式：客户端认证和免客户端认证。聚铭入侵防御系统支持免客户端的Web认证，即通过浏览器就可以完成全部的认证。聚铭入侵防御系统支持本地的用户名/密码的认证外，还支持短信认证、微信认证，还可以结合LDAP、AD域、Radius、POP3等外部服务器实现用户的身份认证。

聚铭入侵防御系统也支持多种认证方式的混合使用，可为不同的用户配置不同的认证方式，实现用户的差异化管理。比如，一部分用户使用本地服务器认证、一部分用户结合LDAP服务器认证，一部分用户不需要进行身份认证。

3.5.6 IP/MAC/VLAN绑定

聚铭入侵防御系统支持二层网络环境和三层网络环境的IP、MAC、IP+MAC和VLAN ID的绑定，可自动阻断非法占用他人IP的用户上网。

3.5.7 跨三层MAC识别

聚铭入侵防御系统支持跨三层MAC识别，用在三层环境下绑定MAC或绑定IP+MAC进行上网认证的实现方式。设备通过配置SNMP服务器地址和MIB信息，通过SNMP协议主动去读取三层交换机上的内网主机的MAC地址。

3.5.8 认证账户有效期

对于一些临时的用户，通过有效期的限定可以控制这些用户的上网时间范围，当用户超出预设的时间有效期，就不能上网。很好的控制了外来用户上网的准入性和上网时长。同时可以设定用户离线多久就自动删除该用户，从而大大的简化了动态用户的管理，增强了用户管理的灵活性。

3.5.9 公用账户

聚铭入侵防御系统的认证账户可支持多人同时登录。如一个员工有两台电脑，那么可以用同一个账户认证，这样两台电脑的流量和行为都记录在同一个账户上，以便统一网络中的流量统计和行为审计与行为分析。

3.5.10 临时账户

支持临时用户自主申请临时账户，方便于外来的临时用户上网使用。支持自动审核和管理员手动审核的核定方法将临时账户加入到组织结构中，从而减少管理员对临时账户的频繁配置，同时统一了临时账户的上网权限和使用期限的管理。

3.5.11 登录重定向

聚铭入侵防御系统支持网页重定向的功能。当用户认证成功后，聚铭入侵防御系统可以将其第一次的Web访问重定向到预设的URL链接。适用于机关、企业集团、大中小学等、或者酒店等网络环境，便于用户上网的时候直接导向最新的公告信息。

3.5.12 单点登录

SSO（单点登录）指如果用户的网络中已经部署有身份认证系统，则本系统可以跟这些身份认证系统进行结合，以识别出某个IP地址上目前正在使用的用户，用户上网时不会再要求先输入用户名/密码，降低对上网用户的影响。包括AD SSO、PPPOE SSO、WEB SSO、RADIUS SSO、第三方设备SSO、HTTP单点登录接口、SSO镜像设置等。

3.5.13 Dkey免审计

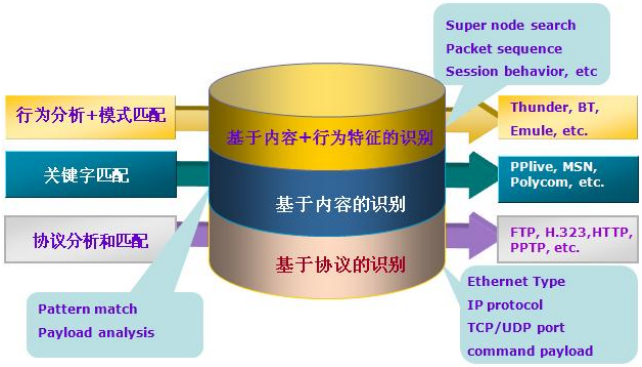
Dkey免审计是指插入Dkey的电脑满足任何一个IP或MAC地址都可以被免除审计。通过在电脑上安装Dkey驱动，需要被免审计的用户通过使用Dkey认证，Dkey通过私有协议和设备通信，将其所有的上网行为免除审计，保障重要部门或是特殊用户的信息安全。

3.6 带宽资源管理

要控制好各种应用，必须首先准确地识别它。传统的安全设备通过IP或者端口封堵各种协议，但这只能局限于网络层和传输层的标准协议，如HTTP、FTP等。P2P、网络游戏、网络电视等一系列应用都是通过协商动态产生的端口，而且诸如电驴、Skype等协议还是加密的，面对这种应用传统的设备无能为力。

以DPI技术为核心，结合基于报文内容及基于行为特征的技术，实现网络中应用的自动识别和智能类。聚铭入侵防御系统可以探测和跟踪动态端口分配，通过比对协议的特征库，能够识别变动端口的流量，并能够对使用同一端口的不同协议进行自动识别。下图是聚铭入侵防御系统识别各种应用采取的方法。

到目前为止，内置的特征库已经支持10000多种协议的识别，并且保持了持续实时的更新。



DPI协议识别

通过精准的协议识别和专业的带宽管理和分配算法，聚铭入侵防御系统提供流量优先级、最大带宽限制、保障带宽、预留带宽、以及随机公平队列等一系列的应用优化和带宽管理控制功能。

3.6.1 流量优先级的划分

聚铭入侵防御系统可基于业务应用的优先级，将业务应用划分为高、中、低等共三个优先级，优先级越高的流量，优先传送。在实现流量控制时，可将核心业务应用、时延要求高的应用、以及重要人物的流量配置为高优先级，同时将P2P、网络电视、WEB视频等非核心的、占用带宽资源较高的应用配置为低优先级。从而可以实现在带宽资源紧张时，优先保证高优先级应用的传送，而在带宽资源使用宽松时，各级应用都可以正常用。

3.6.2 强大的带宽管理功能

通过DPI为核心的深度包检测技术，结合各种应用的行为特点，能够精确到对每个会话的数据包的检测和控制。同时结合流量优先级、随机公平队列等，提供了最大带宽限制、保障带宽、预留带宽等一系列强大的带宽管理功能。

支持源会话数、目的会话数、上行、下行，以及双向总带宽的管理与控制，管理员可以基于线路、流量优先级、源IP地址(地址组、用户组或用户组)、目标IP地址(地址、地址组)、时间、会话、协议和应用等参数对网络流量进行划分，并确定如何有效的、合理的实现带宽的管理与控制。从而实现灵活的带宽控制和应用优化目的。

3.6.3 基于随机公平队列的流量整形和应用优化

基于聚铭入侵防御系统特有的功能，随机公平队列可以保证在相同等级的每一个用户都具有相同的网络资源，避免少部分用户占用了大部分带宽资源的这种极端情况的出现。在相同用户等级的情况下，获得始终如一的服务，使所有用户都满意。

3.6.4 灵活的、强大的基于策略的带宽控制

基于流量优先级、随机公平队列、令牌桶算法、TCP窗口控制算法等技术，提供最大带宽限制、保障带宽、预留带宽的功能，实现灵活、高效、可靠的带宽控制能力。基于策

略的流量控制，可以根据线路、IP地址(组)、用户(组)、协议(组)、URL、时间段等参数配置策略规则，然后再为这些规则分配优先级、带宽、会话数，从而实现对网络中的各种流量进行精细而灵活的控制。最大带宽、保障带宽和预留带宽的详细阐述如下：

- 最大带宽：为某些用户或特定应用指定最大带宽。一方面，防止了某些用户疯狂抢占带宽，保证了网络使用的相对公平性。另一方面，限制了非关键应用毫无节制的消耗宝贵的带宽资源，保证了关键应用的服务质量。
- 保障带宽：结合最大带宽和流量优先级，根据需要为某些关键应用或者VIP客户保障一定带宽。当网络繁忙时，这些关键应用或者VIP客户可以得到预设的保障带宽，并还可以租借空闲的或低优先级流量的带宽；当网络空闲时，低优先级的流量亦可使用当前空闲带宽。从而保证了带宽的合理、高效的使用。
- 预留带宽：为某种特定应用或某些重点客户预留一定带宽，以保证用户在不同时间段、不同的网络使用环境中都能得到同样的带宽管理服务和网络使用感受。

3.6.5 基于单IP/用户的带宽控制

系统不仅提供由IP地址(组)、用户(组)、服务(组)、时间等组合而成的基于策略的带宽控制方式，同时对单IP/用户使用网络资源也提供精细的控制方法。基于单IP/用户的控制，可以将内网的用户分为多种等级，对同等级里的用户实现相同的控制策略。这种方式在对单个主机使用的会话和最大带宽(上行/下行)进行控制的同时，可再对每个主机的多个特定服务(组)的带宽进行精细的控制，再结合时间段，可满足各种复杂的带宽控制需求。

3.6.6 用户限额

为了防止网络资源的滥用和方便管理员管理用户，支持将用户加入黑名单的功能。对进入黑名单的用户可以采取惩罚机制，惩罚期限到了之后，该用户又可以正常使用网络。用户一旦进入黑名单，当再次上网时，网页回弹出已经进入黑名单、是什么原因进入黑名单的。灵活的黑名单功能可以帮助管理员快速、准确的定位出谁肆意占有网络资源。

黑名单可以同时基于以下几种参数来控制：

- 流量配额：控制用户每日、每周、每月使用的流量(上行/下行/双向)总和，防止用户肆意占用带宽。
- 速率控制：控制用户速率(上行/下行)在一段时间不能超过一定阀值。可以防止蠕虫等病毒的突发性、或者防止某个时段某个用户占有大量带宽。
- 并发Session控制：控制用户并发会话数(上行/下行)在一段时间不能超过一定阀值。控制用户滥用P2P、防止病毒等。
- 新建会话控制：控制用户新建会话数(上行/下行)在一段时间不能超过一定阀值。控制用户滥用P2P、防止病毒等。
- 当用户上网参数的超过以上阀值时，即可将用户加入黑名单进行惩罚一定时长（N分钟/小时/天），惩罚方式有以下几种：
- 强制下线：将用户强制下线，即用户不能上网。
- 修改带宽：将用户上网速率修改到较小的值。
- 修改会话：将用户的并发会话数修改到较小的值。

对黑名单的控制，有生效时间，在生效时间内才进行黑名单的控制。在生效时间外，不对用户的速率和会话进行限制，用户产生的流量也不记入黑名单的流量配额内。

3.7 网络特性

3.7.1 路由功能

支持丰富的路由协议，包括静态路由、策略路由、RIP、OSPF、BGP等路由功能，动态路由主要用于和其他设备通过标准的路由协议进行路由交换，在此不展开论述。

3.7.1.1 静态路由

采用了最长匹配原则，同时支持度量值，相同子网匹配之后，度量值小者优先。静态路由还自动检查对应网关物理口的状态，当接口状态down时，该静态路由自动失效，不参与路由匹配。

3.7.1.2 策略路由

策略路由功能强大，本身采用了顺序查找，每条策略内匹配地址则采用了二分排序查找算法，以实现单条策略路由快速匹配。通过快速的条件(源区域、源/目的地址与服务应用）匹配，只要条件匹配成功，策略路由查找就此终止。条件匹配成功后，再判定该策略是否生效(如是否使能、时间计划内外)，优先使用主线路，只有主线路失效的条件下，才启用备用线路，只有线路健康的情况下，才真正成功匹配到策略路由。

3.7.1.3 ISP路由

多外网链路是两个以上的运营商线路时，跨运营商线路互访，由于南北瓶颈，往往造成访问速度明显下降。内置了国内外IP地址池，同时对国内IP进行了细分，形成了电信、联通、网通、铁通和移动地址池，可以通过策略路由引用这些ISP地址池，走相应的线路或者相同运营商线路内负载均衡。

3.7.1.4 应用路由

支持多达10000中网络应用的协议识别，通过应用关联，后续首包可以识别的网络应用，可以路由到相应的线路，将实时业务和非交互网络应用路由至不同服务质量的线路，改善客户对网络应用的用户体验，比如打压大文件下载，提升音视频的网络传输。

3.7.1.5 负载均衡

均衡策略支持源IP轮询、源+目的IP轮询、上行流量、下行流量、总流量、最佳路由和优先线路。其中最佳路径需要根据特定条件使用，它在选路时，首个会话时随机选择一条链路，同时根据配置想所有线路成员发送ICMP或TCP侦测报文，回应最快将记录最佳路径，下次就按照这个记录选择链路。其他的算法比较简单，顾名思义首包就按照相应的权重方式计算或选择线路，往后整个会话都走这条链路。

3.7.1.6 健康检查

多外网链路的负载均衡和备份，都是在建立链路健康检查之上的，失效的线路将不参与负载。支持ICMP/DNS/TCP三种方法的组合健康检查，支持间隔和失效次数可配置，客户视网络状况选择合适的参数和方法，并根据失效次数统计失效千分率，让多个健康检查对象有个明显的直观对比。

3.7.1.7 会话路由

多外网链路主动访问内网，回应报文不能按照路由表或者策略路由来进行，严格遵守源进源出，将这类的路由信息保存在该会话表中，反向回应时直接采用会话发起的网络路径。

3.7.1.8 路由仲裁

配置IP地址时，路由表中生成一条直接路由，优先仲裁。配置的静态路由支持度量值，策略路由支持高低选择，动态路由协议学习到的路由和静态路由公用一张路由表，地位相当于配置的静态路由。路由仲裁顺是：

路由仲裁顺序：直连路由>策略路由(高于任何静态路由)>静态路由(度量值小者优先)>策略路由(低于任何静态路由)；

静态路由仲裁顺序：直连路由优先级最高，其他静态路由先按照掩码最长匹配原则匹配，相同掩码长度根据度量值数值大小匹配，度量值越小优先级越高；

策略路由自上而下匹配，若均衡网关失效，则启用备份网关，两者均无效，则按照仲裁顺序使用其它路由。

3.7.2 NAT功能

3.7.2.1 源地址转换

采用了无锁并行会话表，对代理上网的源地址转换算法进行了优化，完全能满足高并发大流量出口代理上网需求，并可产生会话NAT日志，以满足合规性审计要求。

3.7.2.2 目的地址转换

支持服务映射和一对一两种目的地址转换，采用了会话路由，支持源进源出，内网访问目的地址转换的公网IP自动支持NAT回卷。

3.7.2.3 NAT64与NAT46

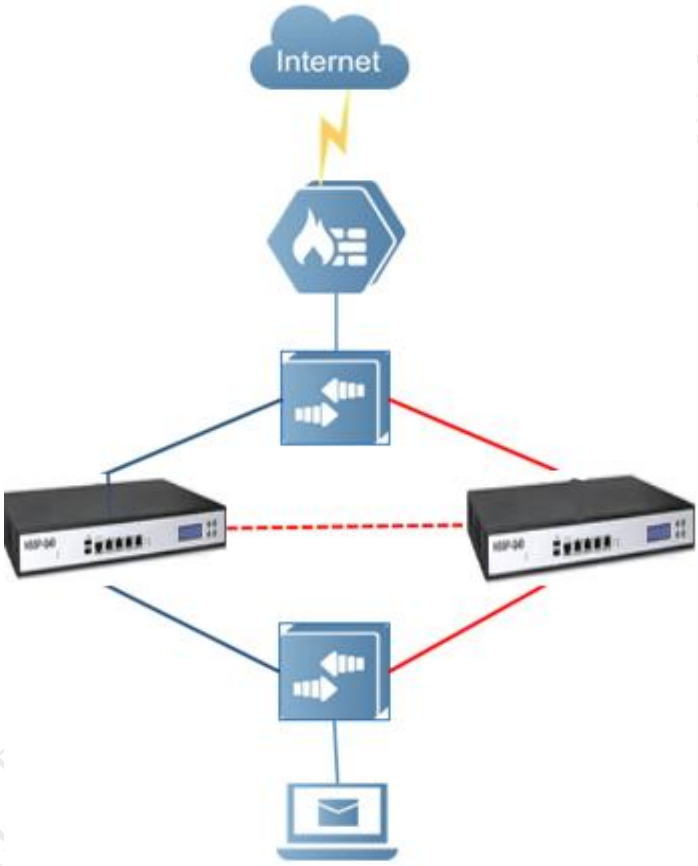
全面支持IPv6网络，过渡阶段支持IPv6与IPv4地址转换功能。

3.7.2.4 会话加速老化

NAT环境下，并发会话的规模将影响新建的效率，设置了高低水位，当会话规模超过高水位，设备将加速会话的老化，当会话规模降至低水位时，又恢复到正常的老化速率，这种会话老化逻辑，适合了大规模网络NAT网络环境的需求。

3.8 高可靠性

3.8.1 网桥模式HA



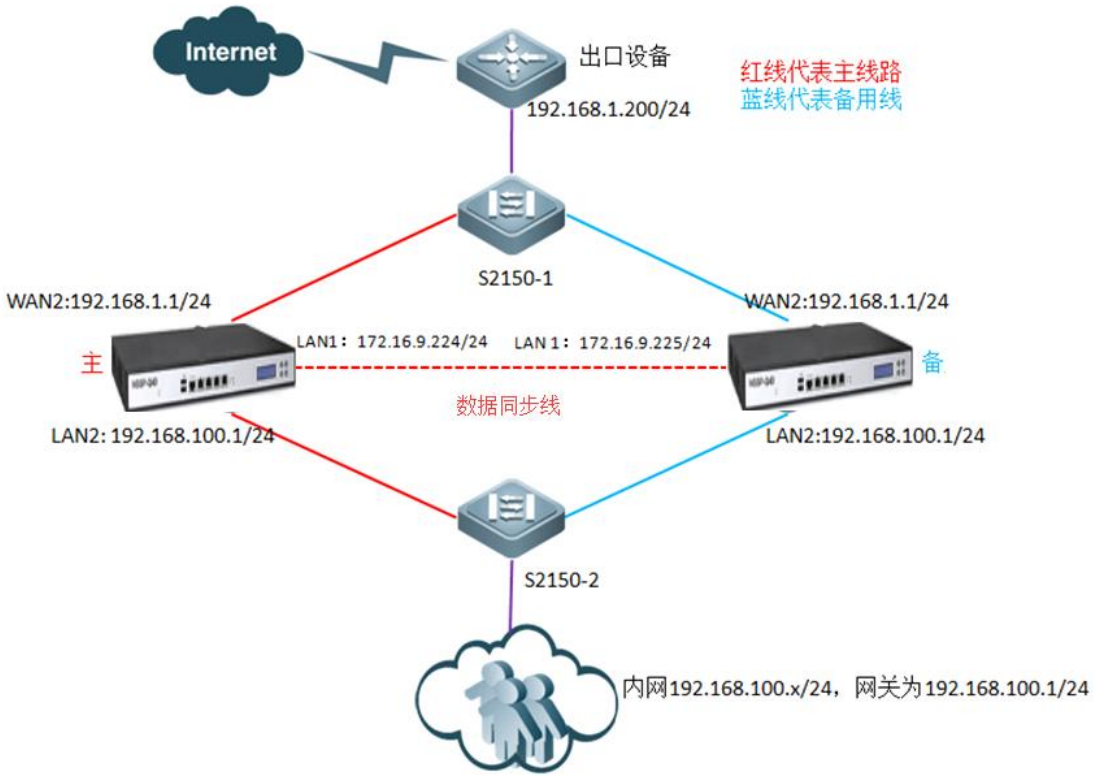
网桥主备HA模式

透明桥接模式下，支持主备方式和桥联动高可靠性功能。

网桥主备HA：如上图所示，网桥模式下，我们选择一个物理口进行HA的状态协商，只有主设备的桥才具备转发功能，从设备不具备转发功能，该部署方式下慎用抢占功能，否则可能导致环路。

桥联动：桥联动功能，利用上下游设备自带HA功能实现，将两台设备分别桥接至上下游HA设备之间，当桥接口发现桥成员一个down了，另一个成员产生联动也down了，这样会促进上下游HA的切换，起到无单点故障功能。

3.8.2 路由模式HA



路由主备HA

路由模式下，支持主备和主主模式高可靠性功能。

路由HA功能是根据VRRP原理实现的，根据两个设备负载工作情景，划分为：

路由主备HA：如上图所示，该模式下只配置1个VRID，所有网络接口都工作在同一个VRRP组中，只有VRRP组的主角色才应答上下游设备的ARP请求，达到路由流量顺利由主设备转发。

路由主主HA：主主HA方式实际是主备HA模式的扩充，它叠加了两个主备HA了。该模式下配置2个VRID，将网络流量横向分割为两个网络，都有自己的上下游，各自的上下游流量分别工作在两个VRRP组中，只有VRRP主角色才应答其上下游设备的ARP请求，达到该VRRP组的流量顺利由其转发。正常情况下，两个VRRP组的主角色分别由两台设备承担，就一台设备来讲，它是一个VRRP组的主角色，同时又是另一个VRRP组的备角色，因而两台设备都是承载流量的，达到了主主HA的效果。

3.9 报表日志

报表中心提供了完整的互联网访问记录，根据IP/用户、应用、时间、线路等参数对威胁日志、用户行为进行全方位的记录，内容I涵盖网络流量、IPS攻击防护、DOS攻击防护、病毒查杀等各种网络威胁和网络行为日志。

由于将所有网络流量和行为记录整合到设备中会影响设备的性能，尤其是对于大量的统计和查询会占用较高的设备资源。另外，为满足网络安全法对日志存储最少要满足180天的要求，除了内置的报表中心，还支持在服务器上安装外置的报表中心。

报表中心提供丰富的统计数据，可按长期(周/月/年)、短期(分钟/小时/日)和实时(秒)的方式显示网络使用状况，并根据用户需求产生报表。从而帮助管理者了解网络整体使用情况。

4 技术优势

4.1 定制操作系统

Linux操作系统是高安全性、高扩展性和可移植的操作系统。对操作系统经过内核裁减，只保留了少数相关的服务与功能，系统内核达到最小化，使操作系统的额外开销与不稳定因素减至最小化。另外，采用特有的文件系统，使系统能抵御突然掉电等物理灾害造成的对系统的损害。

4.2 并行协议栈

对于网络信息安全审计产品来说，数据捕获、协议栈，协议分析等过程中的效率对系统的最后性能起着决定性的因素。

很明显，传统协议栈采用类似函数链的串行处理方式，依次处理以太报文二层处理，IP输入例程和四层输入例程等等，这种传统协议栈存在对CPU的利用不合理的问题。聚铭入侵防御系统系统采用并行协议栈取代传统协议栈，充分发挥SMP架构的性能，给多路CPU、多内核CPU、超线程CPU足够的施展空间。解决并行处理中不可避免的负载均衡的问题，选取硬件分流器中流行的IP+PORT分流策略，将报文分流到并行线程，实现并行协议处理，保证在大流量的情况下处理线程之间工作量均等，有效避免过载线程的出现。采用用户态轮询模式，取消传统协议栈软中断的开销，可以进一步地提高系统的性能。

4.3 特征匹配引擎

内容匹配技术在信息外泄的控制，网络行为分析等方面有重要的作用。而根据每次扫描最多可以发现的关键字的数目，内容匹配算法可以分成单模匹配和多模匹配两种。二者之间的区别在于前者每次扫描后最多可以发现一个关键字，后者则可以发现所有出现的关

键字。现今主要有三种单模匹配算法：KMP、BM、KR。这三种算法的复杂度可以达到O(NM)，N是数据长度，M是关键字数量。

单模匹配算法虽然可以线性地发现数据出现的关键字，但因为其单模的特点，不满足内容审计系统的需要。内容审计系统允许用户配置多个关键字，需要在数据中找到所有出现的关键字的位置，这也是多模匹配算法的长处。因此我们采用了基于状态机的多模匹配算法，对待匹配的数据形成了一个高效的匹配矩阵，只需对数据扫描一遍，就可发现所有出现的关键字。过滤时间与数据长度成正比，和设定的关键字数目无关，算法分析复杂度是O(M+N)，N是数据长度，M是关键字数量。可见此算法对数据长度与及并键字数量具有线性复杂度，比起传统的单模匹配算法大大提高了效率。

4.4 特征库自我管理

经过多年的探索积累，为了适应网络行为的快速变化，系统需要自我维护如下特征库：

IPS库：入侵防御特征规则用来对比检测网络入侵行为的特征，通过完善的检测机制对所有通过的报文进行检测分析，并实时决定允许通过或阻断，内置不同威胁类别的特征规则，管理员根据企业需求自定义特征规则。

病毒库：利用专业的智能感知引擎和不断更新的病毒特征库实现对病毒文件的检测和处理。通过识别和处理病毒文件来保证网络安全，避免由病毒文件而引起的数据破坏、权限更改和系统崩溃等情况的发生。

应用特征库：网络应用特征快速变化，DPI/DFI特征匹配引擎只有及时更新了特征库，才能准确识别应用协议；其实它还包含了过滤审计特征，以满足关键字过滤和一些审计的业务需求。

URL库：URL分类和过滤离不开URL库的更新，系统内置精致的热点URL，中心服务器维护千万级的URL库，以满足高标准客户的需求。

国家/地区IP库：维护了整个IPv4数域的地址库，中国还细分出了不同运营商，策略路由通过引用ISP地址库，实现流量负载优化，规避不同运营商之间“南北互访”瓶颈。

5 典型应用场景

5.1 旁路检测部署

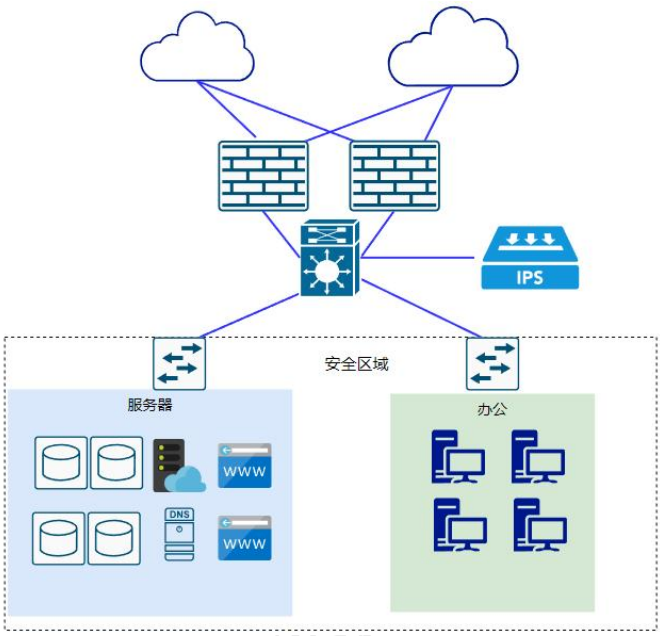
入侵检测设备旁路部署在交换机旁，接收交换机镜像流量进行检测的配置指导，检测威胁流量不干预转发。

大中型企业通常具有以下业务需求如下：

- 企业人员众多，业务复杂，流量构成丰富多样。

- 对网络威胁流量进行监控和管理
- 对设备可靠性要求较高，需要边界设备支持持续大流量运行，即使设备故障也不能影响网络运转。

大中型企业旁路部署检测



5.2 透明模式串联部署

透明部署于企业内联网、互联网网络边界：不改变原有网络拓扑，执行流量的深层次分析和攻击防御，保护子网终端及服务器的安全。