聚铭抗拒绝服务攻击系统
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

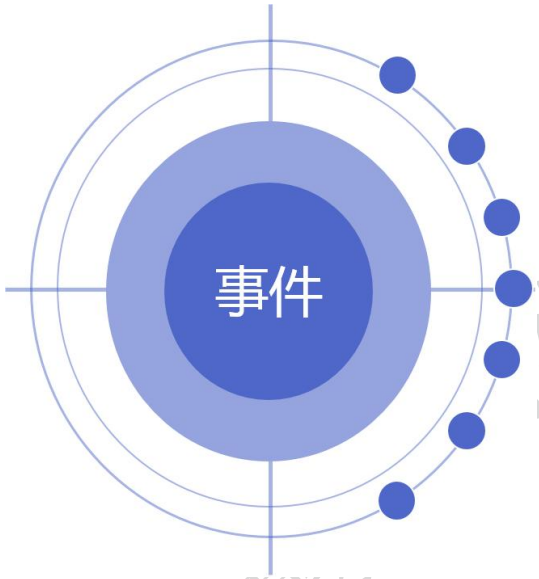
全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

1. 序言

DDoS 攻击是在 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式进行，而 DDoS 则可以利用网络上已被攻陷的计算机作为“僵尸”主机针对特定目标进行攻击。所谓“僵尸”主机即感染了僵尸程序（即实现恶意控制功能的程序代码）的主机，这些主机可以被控制者远程控制来发动攻击。在僵尸主机量非常大情况下（如 10 万甚至更多），可以发动大规模 DDoS 攻击，其产生的破坏力是惊人的。



随着互联网和物联网的发展，DDoS 攻击呈现出新的特点：

- 攻击越来越频繁，流量越来越大

2022 年单次攻击量可以高达 3470Gbps，采用混合 UDP 反射攻击。安全机构监测 2022 年平均每天面对 100Gbps 以上攻击 280 多次。

- 反射放大攻击横扫全球，直接拥塞链路

2022 年世界杯期间，某支付平台从 12 月 3 号 10:10 开始，高强度攻击仅持续 20 分钟，峰值带宽 149Gbps。攻击者通过 UDP Flood 和 UDP 反射持续保持带宽压力的同时，在网络层 CC 基础上增加 SYN Flood、TCP 反射，挑战防御成功率。

- 慢速应用型攻击精确打击互联网金融和游戏等业务系统

2022 年 5 月意大利参议院、上议院、国防部等多个重要政府网站遭到网络攻击，网站无法访问至少 1 个小时。此次攻击使用了“慢速 HTTP”的新型 DDoS 手法，传统防御措施较难抵御，需要针对性处置。

在世界各国对互联网高度依赖的同时，针对大规模网络以拒绝服务攻击为主的恶意行为已经成为互联网上的一个首要安全威胁，几乎每次该类攻击事件都给

整个社会造成了巨大的经济损失，所以保证网络环境有效运行是互联网业务提供商急需解决的重要安全问题，而聚铭抗拒绝服务产品以此为目标，提供强有力的安全保障。

2. DDoS 攻击分析

在网络中,数据包利用 TCP/IP 协议在 Internet 传输,数据包本身是无害的,但是数据包过多,就会造成网络设备或者服务器过载;或者攻击者利用某些协议或者应用的缺陷,人为构造不完整或畸形的数据包,也会造成网络设备或服务器服务处理时间长而消耗过多系统资源,从而无法响应正常的业务。

DDoS 攻击之所以难于防御,是因为非法流量和正常流量是相互混杂的。非法流量与正常流量没有区别,且非法流量没有固定的特征,无法通过特征库方式识别。同时,许多 DDoS 攻击都采用了源地址欺骗技术,使用伪造的源 IP 地址发送报文,从而能够躲避基于异常模式工具的识别。

2.1 DDoS 攻击“主力军”

对现有攻击分析总结,可知常见的 DDoS 攻击有 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、DRDoS、Land Flood、Fragments Flood、Fatboy、DNS Query Flood 和 CC 攻击。

◆ SYN Flood 攻击

利用 TCP 协议缺陷,发送海量伪造的 TCP 连接请求,从而使得被攻击方资源耗尽(CPU 满负荷或内存不足)的攻击方式。

◆ ICMP Flood 攻击

利用海量 ICMP 报文给服务器带来较大的负载,影响服务器的正常服务。由于目前很多抗拒绝服务产品直接过滤 ICMP 报文,因此 ICMP Flood 出现的频度较低,但变种伪造 IP 的 Flood,Smurf 洪水攻击(反射攻击)却愈发猛烈。

◆ Land 攻击

向服务器发送具有 IP 源和目的地址,甚至 TCP 源和目的端口完全一样的伪造的 SYN 包,使服务器创建大量空连接而无法承受这么多流量瘫痪或重启。

◆ CC 攻击

CC 其前身名为 Fatboy 攻击,攻击者借助代理服务器生成指向受害主机的合法请求,实现对服务器资源的恶意消耗。

◆ DNS Query Flood 攻击

利用向被攻击的 DNS 服务器发送海量伪造域名的解析请求，以达到消耗服务器系统资源的目的。

◆ IGMP Flood 攻击

利用 IGMP 协议漏洞(无需认证)，发送大量伪造的 IGMP 数据包造成路由器、抗拒绝服务产品等网关设备内存耗尽，CPU 过载。

以上是最为常见的拒绝服务攻击，随着时间的推移，新的攻击类型及其变种层出不穷。作为专业的 DDoS 解决方案提供商，聚铭时刻关注此类攻击动向，快速制定相应的解决方案，为您的网络安全提供实时的全方位服务。

2.2 DDoS 分类

拒绝服务攻击手段繁多，基于网络协议类型可划分为 TCP 攻击、UDP 攻击、ICMP 攻击、IP 攻击等。其中针对 TCP 的拒绝服务攻击主要有 SYN Flood 攻击、ACK Flood 攻击、CC 攻击、Land 攻击等。针对 UDP 的拒绝服务攻击主要有 UDP Flood、DNS Query Flood 攻击等。针对 ICMP 的攻击主要有 ICMP Flood。针对 IP 的攻击主要有 Fragments Flood 攻击、IGMP Flood 攻击等。

为了便于更好的理解聚铭抗拒绝服务攻击系统的工作原理。聚铭对拒绝服务分为流量型攻击和连接型攻击。

◆ 流量型攻击

通常被攻击的路由器、服务器和防火墙的处理资源都是有限的，而带宽型 DDoS 攻击通过发送海量的包含伪造信息的数据包，造成网络带宽或者设备资源耗尽，从而使正常服务被拒绝。主要包括 SYN Flood、ACK Flood、UDP Flood、ICMP Flood、Fragment Flood 和 NonIP Flood 等。

◆ 应用型攻击

应用型 DDoS 攻击利用诸如 TCP、HTTP 协议的某些特征，使用大量的傀儡机，频繁地连接被攻击设备，形成虚假的客户请求，不断消耗被攻击设备资源；通过不断消耗被攻击设备的有限资源，导致被攻击设备无法处理正常的访问请求。比如 HTTP 半连接攻击和 HTTP Error 攻击就是该类型的攻击。随着代理的出现，应

用型攻击的危害也越来越大。主要包括 CC 攻击、HTTP Get Flood、IDDB 攻击(又称 Logindrv 攻击)、假人攻击等。

2.3 DDoS 攻击发展趋势

聚铭扎根抗拒绝服务攻击领域，多年来通过对国内外拒绝服务攻击情况，实时进行了跟踪分析：

◆ 攻击目的产业化

DDoS 攻击逐渐从偶然攻击动机转变为追求经济利益的谋利手段，如产业竞争、经济敲诈等，并逐渐形成一个成熟的 DDoS 攻击市场及与之相对应的地下产业链。

◆ 攻击手段趋于复杂化

攻击者通过组合多种攻击方式，随机伪造各种正常报文。如攻击包有时随机、有时固定、有时分片；攻击报文长度有时超长、有时超短；宽带型攻击夹带应用型混合攻击。

◆ 攻击目标趋于多样化

从早前攻击针对网络层，消耗链路带宽和被攻击服务器系统资源，演变为针对不同业务特点进行攻击。如慢速向 Web 服务器发送数据查询请求、向游戏服务器发送虚假人物登录请求。

◆ 攻击流量趋于海量化

进入 21 世纪，国内互联网运营商加速宽带网络建设，此后 DDoS 攻击逐渐活跃，单次攻击规模逐年增大。如 2002 年，全球监测到大规模攻击流量不过千兆，而 2014 年监测到单次攻击最高已达到 100G，2020 年 2 月亚马逊网络服务(AWS)成为大规模分布式拒绝服务(DDoS)攻击的目标。其规模为每秒 2.3Tbps。它的数据包转发速率为 293.1 Mpps，每秒请求速率为 694201（rps）。二十年间攻击规模的不断递增，攻击流量海量化已成事实。

3. 常规技术和产品的不足

传统的 DDoS 防御主要是采用为各种不同的攻击行为设置网络流量阈值的方式，这种 DDoS 防御方式有以下几点不足：

配置复杂，自动化不强。传统 DDoS 防御一般要求用户针对某种流量配置相应的阈值，如果对网络及其流量没有清楚的了解，用户很难做出正确的配置。并且，这种用户指定阈值的防御方式也无法根据网络流量的变化动态的对防御规则进行调整。

防御能力比较单一。目前 DDoS 攻击的趋势是多层次和全方位的。在一次攻击过程中，会产生针对半连接的 SYN Flood、UDP Flood 和 ICMP Flood，针对连接的 TCP Connection Flood，以及针对应用层协议的 HTTP Get Flood、HTTP Put Flood 等多种攻击。而传统 DDoS 防御主要针对 SYN Flood 等单一攻击类型，无法应对这种多层次、全方位的攻击，防御能力比较单一。

无法应对未知的攻击。随着 DDoS 攻击工具源代码在网上散播，攻击者可以很容易改变 DDoS 攻击的报文类型，形成 DDoS 攻击的变体。而传统 DDoS 防御主要针对已知 DDoS 攻击，对未知的 DDoS 攻击变体无法进行防御。

3.1 技术防护的不足

- 安全策略

路由器的一些安全策略，如 ACL(访问控制列表)、QoS(服务质量)、黑洞路由等，可以对非法的流量进行过滤和对优先服务提供保证。比如 ACL 等，这些措施从某种程度上确实可以过滤掉非法流量，一般来说，ACL 可以基于协议或源地址进行设置。比如设置只允许 TCP 端口访问，可以一定程度上防护 UDP Flood 攻击，但是目前较多的 DDoS 攻击采用的是常用的一些合法协议，比如 http 协议，这种情况下，路由器就无法对这样的协议进行过滤。同时，如果 DDoS 攻击采用伪造 IP 地址方式进行攻击，ACL 就无法根据源地址进行防护。路由器还有一些功能，比如黑洞路由方式进行防护攻击，这种方式相当于直接屏蔽掉对被攻击

IP 的访问，但在目前市场竞争激烈的情况下，这种做法无疑会流失一定的用户量。

◆ 资源扩容

对于用户来说，为了防御 DDoS 攻击，有些客户可能会通过多台冗余设备，或者增加多条链路来提高网络系统防护能力。对于运营商或 IDC 提供商来说，可能会通过扩大链路带宽的方式来增加防护能力，但这些都只是一种类似“妥协”的手段，无法从根本上去防御 DDOS 攻击。一方面会造成成本成倍增加，另一方面，如果攻击者同样提高攻击流量，同样会造成这种防御的方法彻底失效，长期下来会导致用户体验下降，用户资源流失。

◆ uRPF

uRPF 是一种单播反向路由查找技术，用于防止基于源地址欺骗的网络攻击行为。uRPF 通过检查数据包中源 IP 地址，根据接收到数据包的接口和路由表中是否存在源地址路由信息条目，来确定流量是否真实有效，并选择数据包是转发或丢弃。通信网络中，诸如 DoS 攻击、TCP SYN 洪泛攻击、UDP 洪泛攻击和 ICMP 洪泛攻击等，都可能通过借助源地址欺骗的方式攻击目标设备或者主机，造成被攻击者系统性能严重的降低，甚至导致系统崩溃。uRPF 技术就是网络设备为了防范此类攻击而使用的一种常用技术。但是 uRPF 防护的是非本子网发出的伪造源 IP 地址数据包，如果攻击者攻击采用本子网 IP 地址作为源 IP 地址，uRPF 无法防御。

3.2 产品防护的不足

传统的网络安全产品的种类非常多，但对 DDoS 攻击防护却表现得非常薄弱。传统的抗拒绝服务产品、入侵检测系统、路由器和交换机等，因其设计之初并未考虑对 DDoS 的防护，而不能全面的对 DDoS 攻击进行有效检测和防护。

◆ 传统防火墙设备

防火墙产品是我们比较常用的网络安全设备，通过 NAT 隐藏内部网络结构，设置 DMZ 区(非军事化区)保护内部网络，三层数据包过滤非法数据。虽然有些防火墙内置了某些模块能够对攻击进行检测，但这些检测机制一般都是基于特征规则，DDoS 攻击者只要对攻击数据包稍加变化，防火墙就无法应对，对 DDoS 攻击

的检测必须依赖于行为模式的算法。另一个原因是传统防火墙计算能力的限制，传统的防火墙是以高强度的检查为代价，检查的强度越高，计算的代价越大。而DDoS 攻击中的高流量会造成防火墙性能急剧下降，不能有效地完成包转发的任务。而防火墙最主要的功能是提供内网网络访问外网的功能，主要是 NAT、VPN 服务等。这样防火墙的性能将成为瓶颈，如果防火墙遭到 DDoS 攻击防火墙性能下降，将导致整个网络陷入瘫痪。

- IPS/IDS

IPS/IDS 作为当前网络攻击防御和检测的有力工具，主要基于特征规则库检测阻断攻击。但是常见的 DDoS 攻击多以合法的数据包进行流量攻击，这样 IPS/IDS 就很难通过规则对这些攻击进行检测。

4. 聚铭抗拒绝服务攻击系统

聚铭通过多年的发展以及在抗拒绝服务产品研发、生产和部署中，形成了具有自主知识产权、性能优越、品质优秀的聚铭抗拒绝服务系统，可为您的信息系统提供完善的安全保护。一流的核心模块，高效的防护算法使得本系列产品成为抗拒绝服务的防护聚铭。

4.1 防御架构

聚铭抗拒绝服务攻击系统采用智能的自适应多层次防御架构对 DDoS 攻击进行检测和防御。该架构采用验证、分析等方法标识出可疑流量，并针对可疑流量做一系列的验证和防御。

1.过滤规则模块

过滤规则包括静态过滤规则和动态过滤规则：静态过滤规则是由用户手动配置的；动态过滤规则是由异常流量识别模块和异常应用识别模块通过流量统计、行为分析等方法发现可疑流量后动态添加的。

过滤规则模块根据过滤规则对流量进行过滤，将已经确定是攻击的流量进行阻断；将可疑的流量交给动态验证模块进行动态验证。

2.动态验证模块

动态验证模块采用各种方法对通过过滤规则模块的流量进行动态验证，阻止源地址欺骗的报文通过。所采用的动态验证方法例如：针对 HTTP 请求采用 HTTP 重定向方法；针对 DNS 请求采用 DNS 重定向方法。

3.异常流量识别模块

异常流量识别模块对通过过滤规则模块和动态验证模块的流量进行统计，并与已经获得的学习流量基线进行比较。如果超出，则生成动态过滤规则，从而使过滤规则模块根据生成的动态过滤规则对后续流量进行过滤。

学习流量基线是指保护对象在正常业务运行状态下的流量信息模型。如果网络流量超出学习流量基线，则说明网络中可能存在异常，需要对其进行验证和确认。

4.应用异常识别模块

应用异常识别模块针对不同的应用协议，对通过过滤规则模块和动态验证模块的应用层流量（如 HTTP Error 攻击等）进行深入分析。如果发现有异常流量，则生成动态过滤规则，从而使过滤规则模块根据生成的动态过滤规则对后续流量进行过滤。

5.带宽控制模块

各种流量如果通过了上述模块，表明数据报文是正常的，但仍有可能出现流量过大导致保护对象过载的情况。通过带宽控制模块，可以对要流入保护对象的流量进行带宽限制，保证保护对象不会过载。

4.2 功能一览

聚铭抗拒绝服务攻击系统产品，功能丰富，界面简洁，便于管理。概括起来有以下主要功能和技术优势：设备均采用主动探测防护模式，防护更加主动、人性、精准，DFI+DPI 结合的数据包分析识别技术，更加丰富多样的 DDoS 攻击防护策略、灵活进行多种防护手段的随意切换，更加详尽的应用层协议及端口保护，对更多的特殊应用的定向保护，更加丰富、人性化的数据包规则过滤，丰富多样的审计报表格式，人性化的设备需求 DIY 定制，丰富多样的部署方式、支持各种网络环境的部署等。

◆ 精确智能的攻击检测及防护

聚铭抗拒绝服务攻击系统，应用了自主研发的抗拒绝服务攻击算法，拥有智能参数阀值，对 SYN Flood、UDP Flood、ICMP Flood、IGMP Flood、ACK Flood、DNS Query Flood、Ping Sweep 等流量型攻击，HTTP Proxy Flood、HTTP Get Flood、CC Proxy Flood、Connection Exhausted 等连接型攻击和 Smurf、Land-based、Teardrop、Fragment Flood、Red Code 等漏洞型攻击，及其他各种常见的攻击行为均可有效识别，并通过集成的机制实时对这些攻击流量进行阻断处理，保障业务系统正常运行。内置各种针对网站、网络游戏、音视频聊天室等专门的 Web 防护插件及游戏防护插件，彻底解决针对此类应用的 DDoS 攻击。

◆ 简洁丰富的 WEB 管理

聚铭抗拒绝服务攻击系统，具有丰富的设备管理功能，基于简洁的 Web 管理方式，支持本地或远程升级。丰富的日志和审计功能也极大地增强了设备的可用性，不仅能够针对攻击进行实时监测，还能对攻击的历史日志进行方便的查询和统计分析，便于对攻击事件进行有效的跟踪和追查。整个 Web 界面主要有状态监控、攻击防御、日志分析、系统配置和服务支持五个模块。

◆ 专业健全的连接跟踪机制

聚铭抗拒绝服务攻击系统，内部实现了完整的 TCP/IP 协议族，具有强大的连接跟踪能力。每个进出的连接，抗拒绝服务产品都会根据其源地址进行分类，并显示出来给用户，方便用户对受保护主机状态的监控。并且提供了连接超时，重置连接等辅助功能，弥补了 TCP/IP 协议族本身的不足，使您的服务器在面对拒绝服务攻击中游刃有余。

◆ 通用方便的报文规则过滤

聚铭抗拒绝服务攻击系统，除了提供专业的 DoS/DDoS 攻击检测及防护外，还提供了面向报文的通用规则匹配功能，可设置的包括 IP 地址、端口、TCP 标志位、关键字、协议等，极大的提高了通用性及防护力度。系统中还内置了若干预定义规则，易于使用。

◆ 便捷快速的抓包取证功能

聚铭抗拒绝服务攻击系统，内置抓包工具，具有数据包捕获功能，依据自行设置的条件启动抓包任务，针对 DoS/DDoS 攻击，获取符合抓包条件的网络数据包，为电子取证提供依据。

◆ 完善强大的模块防护功能

聚铭抗拒绝服务攻击系统具有完善的连接跟踪机制，准确的应用层协议过滤。应用层协议高级防护，如对 FTP、SMTP、POP3、HTTP 等应用服务的保护。数据包规则过滤可对端口和 TCP 的 SYN、FIN、PSH、ACK 等标志位过滤。数据包内容细致过滤可对数据包内关键字过滤并支持明文和十六进制格式。聚铭抗拒绝服务系统还可以实现数据包捕获功能、单 IP 流量限制、SNMP 管理、支持查询 CPU 内存利用率和接口流量及系统健康状态等。

◆ IPV4/IPV6 混合网络功能

针对 IPv6 越来越多的普及，运用 IPv4 与 IPv6 的双栈兼容技术，对网络中巨大的数据量进行深度的分析清洗，提取受保护服务器与众多客户端的通信进行数据统计，发现数据中的攻击特征；运用流量防护模块、WEB 防护模块、GAME 防护模块、DNS 防护模块、语音防护模块等高效的模块化防护技术，对攻击流量进行处理、过滤，再将纯净的流量转发给服务器，从而保护网络的正常使用。同时，提供给用户全面的日志、报表输出功能，为网络管理员在日常的管理和对网络安全的判断提供详细的依据。

4.3 系统防护原理

聚铭抗拒绝服务系统系列产品是基于嵌入式系统设计的，其在系统核心实现了防御拒绝服务攻击的算法，创造性地将算法实现在协议栈的最底层，避开了 IP/TCP/UDP 等高层系统网络堆栈的处理，使整个运算代价大大降低。自主研发的高效防护算法，效率极高。

聚铭抗拒绝服务攻击系统主要采用了攻击检测、主机识别、指纹识别、协议分析、攻击过滤、流量控制、端口保护、连接控制、连接跟踪和日志审计来达到拒绝服务攻击的防护。

◆ 攻击检测

利用了多种技术手段对 DoS/DDoS 攻击进行有效的检测，在针对不同的流量触发不同的保护机制，提高效率的同时确保准确度。

◆ 主机识别

聚铭抗拒绝服务攻击系统可自动识别其保护的各个主机及其地址，某些主机受到攻击不会影响其它主机的正常服务。

◆ 指纹识别

用来识别整个连接过程，其中包括：源、目的、协议、端口等情况的识别。

◆ 协议分析

聚铭抗拒绝服务攻击系统采用了协议独立的处理方法，对于 TCP 协议报文，通过连接跟踪模块来防护攻击；而对于 UDP 及 ICMP 协议报文，主要采用流量控制模块来防护攻击。

◆ 攻击过滤

攻击过滤为默认模式，此模式下，运行完整的攻击过滤流程，过滤攻击保证正常流量到达主机。

◆ 流量控制

主要是针对一些攻击流量做限制。紧急触发状态，针对攻击频率较高的攻击防护模式，此模式将更为严格过滤攻击。简单过滤流量限制，是针对某些显见的攻击报文做的一种过滤模式，目前可以过滤内容完全相同的报文，及使用真实地址进行攻击的报文。忽略主机流量限制，用于限制忽略主机的流量，当某个忽略主机的流量超过设置值，超过的流量将被丢弃。伪造源流量限制，用于限制内网攻击。当某数据包的源 MAC 地址不同于记录到的 MAC 地址，该数据包将被认为是伪造源流量，超过设置值的伪造源流量将被丢弃。

◆ 连接控制

根据攻击的流量和连接数阀值来设置触发防护选项，连接数阀值可以根据不同情况来灵活控制。

◆ 连接跟踪

聚铭抗拒绝服务攻击系统针对进出的连接均进行连接跟踪，并在跟踪的同时进行防护，彻底解决针对 TCP 协议的各种攻击。

◆ 日志审计

日志记录可全面记录产品系统运行及防护状态，并对不同权限的操作进行记录。

5. 亮点选择

通过多年市场发展，聚铭抗拒绝服务攻击系统拥有独立自主的技术专利，专业的硬件平台架构和线速处理技术，专用的安全操作系统，广泛的行业合作对象，优秀专业的技术和系统的服务优势。

5.1 专业的技术团队

聚铭安全实验室研究世界先进的安全技术和安全产品，不断跟踪最新的黑客工具和黑客攻击技巧，执着专注的攻防研究人员构筑成安全服务队伍的强大技术后盾。研发部、测试部、网络工程部、售后中心各部门在统一领导下合作开展工作。

聚铭拥有一支掌握先进安全理念和成熟安全技术的安全服务队伍，有众多技术人员，拥有 CISP、CISAW、CCIE、HCIE 等技术，有着丰富的安全咨询、安全系统集成、专业安全服务经验，并熟悉用户业务应用和了解安全隐患所在。聚铭将竭其在信息安全领域的造诣，帮助用户评估信息系统的安全状况，指导用户进行信息安全体系建设，提高用户的安全意识和技术水平，实现业务安全目标。

5.2 高端硬件架构

聚铭抗拒绝服务系统采用专业的硬件架构，使用了目前先进的 ATCA 架构硬件平台，在背板结构上，结合独创的攻击检测算法，能够针对海量 DDoS 进行防护。ATCA 支持星状、网状、双星和两组双星等多种拓扑结构，为用户提供更多接口选项，具备更丰富的弹性；在多板卡间数据传输问题上，ATCA 采用全网状结构，使内部最高数据传输交换速率达 2.4Tbps；在背板总线协议选择上，ATCA 支持多种基于数据包的交换式总线； ATCA 规范在外形设计定义上预留了更大的空间，同时提供了冗余风扇和温度监控管理，以增强系统散热能力；ATCA 代表着全开放、模块化的工业标准，它可以使设备制造商采用第三方厂商的可互操作性、成熟的商业化（COTS）软硬件组件，在快速实现集成或升级换代的同时，增强了系统的整体兼容性。

由于系统支持旁路部署方式，可对 DDoS 攻击流量进行牵引，同时通过部署若干台聚铭设备形成集群，更加增强了系统抵御巨大规模的 DDoS 攻击的能力，保证了正常流量的顺畅通过。

5.3 硬件平台国产化

信息安全和国产化已经是国家战略，各种国产化的政策相续出台，要求核心单位优先使用安全可控的国产化网络管理软件。聚铭除了软件上使用自主研发的抗拒绝服务攻击系统，同时在硬件平台上选用了国内的海光和飞腾平台，提高设备自身的安全可信度。

5.4 独立自主的技术

◆ 独特的连接代理防护算法

聚铭抗拒绝服务系统系列产品中应用了自主研发的抗拒绝服务攻击算法。针对 SYN 攻击，采用 SYN Proxy 连接代理防护模式，以代理模式处理客户端与服务器之间的连接，同时完成攻击报文的过滤，即使在海量攻击下仍然可以保证 99.99%的新建连接的连接成功率。

◆ 高效的连接数据转发算法

聚铭抗拒绝服务系统系列产品，采用自主研发的 TCP Fast Rechecksum 技术，高效的处理来自 TCP 的连接数据及其校验和，并进行快速转发，而无需重新统计报文数据。

◆ 模块化的内核防护算法

聚铭抗拒绝服务系统系列产品，采用了 Kernel Protection Plugin For Linux &Windows 技术，将特定的防护算法以模块的形式实现，简化了核心代码，优化了系统构架，并具有良好的扩展性。

◆ 基于页面插入式的 WEB 防护算法

聚铭抗拒绝服务系统系列产品，采用 Web Protection Based On Page Injection 即基于页面插入式 Web 防护算法。对于开启防护的 Web 服务器，防护模块会主动插入 Web 页面，客户端可无察觉的自动完成验证过程，已达到高效

的防御 Web 类连接攻击的目的。另外，也可以通过验证服务器辅助来加强防护级别。

◆ 基于数据挖掘的通用防护算法

聚铭抗拒绝服务系统系列产品，采用 Generic Protection Based On Data Mining 技术即基于数据挖掘的通用防护算法，对于开启保护的服务器，防护模块会自动对客户端与服务器端的通信进行数据统计与挖掘，察觉恶意流量并加以过滤，有效率高达 97.3%以上。

◆ 可扩展的集群模式

聚铭抗拒绝服务系统系列产品，采用 Extensible Firewall Cluster Mode 即可扩展的集群模式，通过领先的数据分流技术，使得若干设备可组合形成更大的防护主体，提供海量攻击的防护解决方案。

◆ 多平台架构支持及内核防盗版技术

聚铭抗拒绝服务系统系列产品，支持多核、NP、ATCA 架构，拥有百兆级、千兆级、万兆级多种防护级别的产品。同时采用 Anti-Cracking Mechanism In Kernel 技术，实现对系统核心的加密技术，使得本系统具有很强的防盗版、防拷贝能力。

◆ 灵活多样的部署方式

聚铭抗拒绝服务系统系列产品，支持 IEEE802.3AD 和 IEEE802.1Q 等其他路由交换协议。具备多种环境部署能力，能在不改变现有网络拓扑的情况下，以透明模式接入。支持多种部署方式，如分布式部署、双机热备部署、集群部署和旁路部署等。

5.5 专业的服务

◆ 广泛的行业解决方案

针对不同的客户，抗拒绝服务攻击所面临的网络环境也不同，政企网、IDC、ICP 和 ISP 等多种网络环境并存，给抗拒绝服务系统的部署带来了不同的挑战。通过近十年的发展，聚铭抗拒绝服务攻击系统已经广泛部署应用于不同的行业，如互联网、运营商、证券、电力、医疗、社保、税务和教育等行业，积累了大量

的行业解决方案与经验，使您不必为本网络的安全解决方案而苦恼，只要您一个电话，剩下的事由聚铭来做。

◆ 全面系统的专业培训服务

聚铭强大的服务体系，为您的网络安全将提供全方位的服务。凡是使用聚铭系列产品均会得到聚铭为您量身定制的网络安全专业培训，除了针对抗拒绝服务知识与聚铭产品操作的培训，我们还将为您提供一系列扩展培训，使您对网络安全有更全面的了解。

◆ 优质的售后服务体系

使用聚铭抗拒绝服务攻击系统，质保期内您将享有免费升级服务。除了为您提供更便捷、更有保障的产品售前咨询和售中服务，我们强大的专业技术团队还将为您提供全方位的售后技术支持。我们的客服中心和技术支持中心为您提供7x24 小时的专业服务。定期为产品系统更新，随呼随到的在线技术支持以及紧急的现场支持，使您的网络始终保持在最安全的状态，免除您的后顾之忧。我们的服务宗旨是：客户至上，服务第一。

◆ 量身的模块定制服务

聚铭抗拒绝服务攻击系统，内置的协议自定义模块，可以随着网络应用的变化进行方便的修改，即对各种特殊应用进行自定义防护，如用户自行开发的某些聊天室、游戏服务等。聚铭抗拒绝服务系统也将根据您的实际应用进行开发，实现模块量身定制。