铱迅信息
yxlink.com

# 铱迅抗拒绝服务系统

# 产品白皮书

南京铱迅信息技术有限公司

Nanjing Yxlink Information Technologies Co.,Ltd.

# *注意*

本手册没有任何形式的担保、立场表达或其他暗示。若有任何因本手册或其所提到之产品信息，所引起直接或间接的数据流失、利益损失或事业终止，铱迅信息不承担任何责任。

铱迅信息保留可随时更改手册内所记载之硬件及软件规格的权利，而无须事先通知。

本公司已竭尽全力来确保手册内载之信息的准确性和完善性。如果您发现任何错误或遗漏，请向铱迅信息反映，对此，我们深表感谢。

## *商标信息*

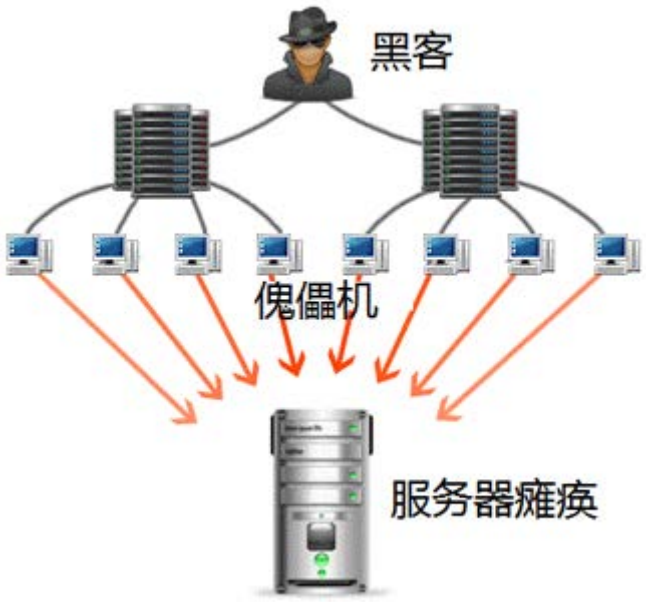
铱迅信息、铱迅抗拒绝服务系统的标志为南京铱迅信息技术有限公司的商标或注册商标。本手册或随铱迅信息产品所附的其他文件中所提及的所有其他商标名称，分别为其相关所有者所持有的商标或注册商标。

# 目录

# 一、概述

## 1.1 DDOS 攻击场景

怎么判断网络正遭受到DDOS攻击呢？一般来说，被攻击主机上有大量等待的TCP连接，网络中充斥着大量的无用的数据包，源地址为假，制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯。利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求，严重时会造成系统死机等等，这些都是遭受到 DDOS 攻击时的场景。




最经典的攻击是 synflood 攻击，它利用 TCP/IP 协议的漏洞完成攻击。通常一次 TCP 连接的建立包括 3 个步骤，客户端发送 SYN 包给服务器端，服务器分配一定的资源给这里连接并返回 SYN/ACK 包，并等待连接建立的最后的 ACK 包，最后客户端发送 ACK 报文，这样两者之间的连接建立起来，并可以通过连接传送数据了。而攻击的过程就是疯狂发送 SYN 报文，而不返回 ACK 报文，服务器占用过多资源，而导致系统资源占用过多，没有能力响应别的操作，或者不能响应正常的网络请求。

这个攻击是经典的以小搏大的攻击，自己使用少量资源占用对方大量资源。一台普通的 Linux 系统大约能发到 30－40M 的 64 字节的 synflood 报文，而一台普通的服务器 20M 的流

量就基本没有任何响应了。而且 synflood 不仅可以远程进行，而且可以伪造源 IP 地址，给追查造成很大困难，要查找必须所有骨干网络运营商，一级一级路由器的向上查找。

## 1.2 DDOS 攻击分析

DDOS 是英文 Distributed Denial of Service 的缩写，意即“分布式拒绝服务”，DDOS 的中文名叫分布式拒绝服务攻击，俗称洪水攻击。

DDOS 攻击手段是在传统的 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的，当攻击目标 CPU 速度低、内存小或者网络带宽小等等各项性能指标不高时，它的效果是明显的。

随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DOS 攻击的困难程度加大了。目标对恶意攻击包的消化能力加强了不少，例如攻击软件每秒钟可以发送 3,000 个攻击包，但我的主机与网络带宽每秒钟可以处理 10,000 个攻击包，这样一来攻击就不会产生效果。这时候分布式的拒绝服务攻击手段（DDOS）就应运而生了。如果说计算机与网络的处理能力加大了 10 倍，用一台攻击机来攻击不再能起作用的话，攻击者使用 10 台攻击机同时攻击呢？用 100 台呢？DDOS 就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。

高速广泛连接的网络给大家带来了方便，也为 DDOS 攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以 G 为级别的，大城市之间更可以达到几百上千 G 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以在分布在更大的范围，选择起来更灵活了。

## 1.3 传统的 DDOS 防御的不足

### 1.3.1 配置复杂，自动化不强

传统 DDOS 防御往往要求用户针对某种流量配置相应的阈值，如果对网络中的流量不清楚的话，用户很难做出正确的配置。

### 1.3.2 防御能力比较单一

传统 DDOS 防御主要针对 SYN Flood 等单一攻击类型进行防御，能力比较单一。现在 DDOS 攻击的趋势是多层次和全方位的，在一次攻击攻击过程中，会产生针对网络层的 SYN、UDP 和 ICMP Flood，针对连接的 TCP connection Flood，和针对应用层协议的 HTTP GET、PUT Flood。

### 1.3.3 无法区分异常流量

传统 DDOS 防御对于检测到的流量异常后，无法做进一步的区分，而只是简单的将所有异常流量全部丢弃，导致合法用户的请求也得不到响应。

### 1.3.4 无法应对未知的攻击

传统 DDOS 防御主要针对已知 DDOS 攻击，而随着 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。

# 二、产品简介

铱迅抗拒绝服务系统（英文：Yxlink Anti-DDOS System，简称：Yxlink ADS）是铱迅信息结合多年在网络攻击理论与拒绝服务攻击实践的基础上，自主研发的一款独特抗拒绝服务系统，可高效防御 DOS/DDOS 攻击中 SYN Flooding 攻击、Ping of Death、UDP Flooding 攻击等多种未知攻击。


该产品致力于解决网络过载带来干扰甚至阻断正常的网络通讯的安全问题，广泛适用于“政府、金融、运营商、公安、能源、税务、工商、社保、交通、卫生、教育、电子商务”等所有涉及网络应用的各个行业。部署铱迅抗拒绝服务系统产品，可以帮助用户有效识别各种常见的攻击行为，并通过集成的机制实时对这些攻击流量进行检测及阻断，具备远处网络监控和数据包分析功能，能够迅速获取、分析最新的攻击特征，防御最新的攻击手段。

# 三、铱迅抗拒绝服务系统

## 3.1 产品功能

### 3.1.1 DDOS/DOS 攻击过滤

DDOS 攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。如果说以前网络管理员对抗 DOS 可以采取过滤 IP 地址方法的话，那么面对当前 DDOS 众多伪造出来的地址则无计可施。常见的 DOS/DDOS 攻击类型如下：

*Ping of Death:*

许多操作系统的 TCP/IP 协议栈规定 ICMP 报文大小为 64KB，并为此分配缓冲区。Ping of Death 故意产生畸形报文，声称自己的大小超过 64KB，使得协议栈出现内存分配错误，导致死机。

*Teardrop:*

攻击利用 UDP 包重组时重叠偏移的漏洞，对系统主机发动拒绝服务攻击，最终导致主机若掉。

*UDP flood:*

又称 UDP 洪水攻击或 UDP 淹没攻击，UDP 是没有连接状态的协议，因此可以发送大量的 UDP 包到某个端口，如果是个正常的 UDP 应用端口，则可能干扰正常应用，如果是没有正常应用，服务器要回送 ICMP，这样则消耗了服务器的处理资源，而且很容易阻塞上行链路的带宽。常见的情况是利用大量 UDP 小包冲击 DNS 服务器或 Radius 认证服务器、流媒体视频服务器。100k pps 的 UDPFlood 经常将线路上的骨干设备例如防火墙打瘫，造成整个网段的瘫痪。

*TCP SYN 泛洪攻击:*

一个正常的 TCP 连接需要进行三方握手操作。首先，客户端向服务器发送一个 TCP SYN 数据包而后，服务器分配一个控制块，并响应 一个 SYN ACK 数据包。服务器随后将等待从

客户端收到一个 ACK 数据包。如果服务器没有收到 ACK 数据包，TCP 连接将处于半开状态，直到服务器从客户端收到 ACK 数据包或者连接因为 time-to-live(TTL)计时器设置而超时为止。在连接超时的情况下，事先分配的控制块将被释放。当一个攻击者有意地、重复地向服务器发送 SYN 数据包，但不对服务器发回 SYN ACK 数据包答复 ACK 数据包时，就会发生 TCP SYN 泛洪攻击。这时，服务器将会失去对资源的控制，无法建立任何新的合法 TCP 连接。

## *Smurf 攻击：*

攻击者会向接收站点中的一个广播地址发送一个 IP ICMP ping(即“请回复我的消息”)。Ping 数据包随后将被广播到接收站点的本地网络中的所有主机。该数据包包含一个“伪装的”源地址，即该 DoS 攻击的对象的地址。每个收到此 ping 数据包的主机都会向伪装的源地址发送响应，从而导致这个无辜的、被伪装的主机收到大量的 ping 回复。如果收到的数据量过大，这个被伪装的主机就将无法接收或者区分真实流量。

## *Stacheldraht：*

Stacheldraht 基于客户机/服务器模式，其中 Master 程序与潜在的成千个代理程序进行通讯。在发动攻击时，侵入者与 master 程序进行连接。Stacheldraht 增加了新的功能：攻击者与 master 程序之间的通讯是加密的，对命令来源做假，而且可以防范一些路由器用 RFC2267 过滤，若检查出有过滤现象，它将只做假 IP 地址最后 8 位，从而让用户无法了解到底是哪几个网段的哪台机器被攻击；同时使用 rcp (remote copy，远程复制)技术对代理程序进行自动更新。Stacheldraht 同 TFN 一样，可以并行发动数不胜数的 DoS 攻击，类型多种多样,而且还可建立带有伪装源 IP 地址的信息包。Stacheldraht 所发动的攻击包括 UDP 冲击、TCP SYN 冲击、ICMP 回音应答冲击等。

铱迅抗拒绝服务系统可以对网络中的流量做实时的分析，自动过滤非法的攻击流量，让合法的流量能够顺利通过。

### 3.1.2 CC 攻击过滤

CC 攻击主要针对 WEB 应用程序比较消耗资源的地方进行疯狂请求，比如，论坛中的搜索功能，如果不加以限制，任由人搜索，普通配置的服务器在几百个并发请求下，MYSQL 服务就挂掉了。

想要防御 CC 攻击，就要知道它的的种类有三种，直接攻击，代理攻击，僵尸网络攻击。

直接攻击主要针对有重要缺陷的 WEB 应用程序，一般说来是程序写的有问题的时候才会出现这种情况，比较少见。僵尸网络攻击有点类似于 DDOS 攻击了，从 WEB 应用程序层面上已经无法防御。

CC 攻击者一般会操作一批代理服务器,比方说 100 个代理,然后每个代理同时发出 10 个请求，这样 WEB 服务器同时收到 1000 个并发请求的，并且在发出请求后，立刻断掉与代理的连接，避免代理返回的数据将本身的带宽堵死，而不能发动再次请求，这时 WEB 服务器会将响应这些请求的进程进行队列，数据库服务器也同样如此，这样一来，正常请求将会被排在很后被处理，这时就出现页面打开极其缓慢或者白屏。

传统的手段很难防止 CC 攻击，因为 CC 攻击来的 IP 都是真实的，分散的，而且 CC 攻击的数据包都是正常的数据包，全都是有效的请求，无法拒绝的请求。

铱迅抗拒绝服务系统可以精确到 URL 级别对 CC 攻击进行探测拦截，自动探测代理服务器洪水攻击，并有效进行过滤。

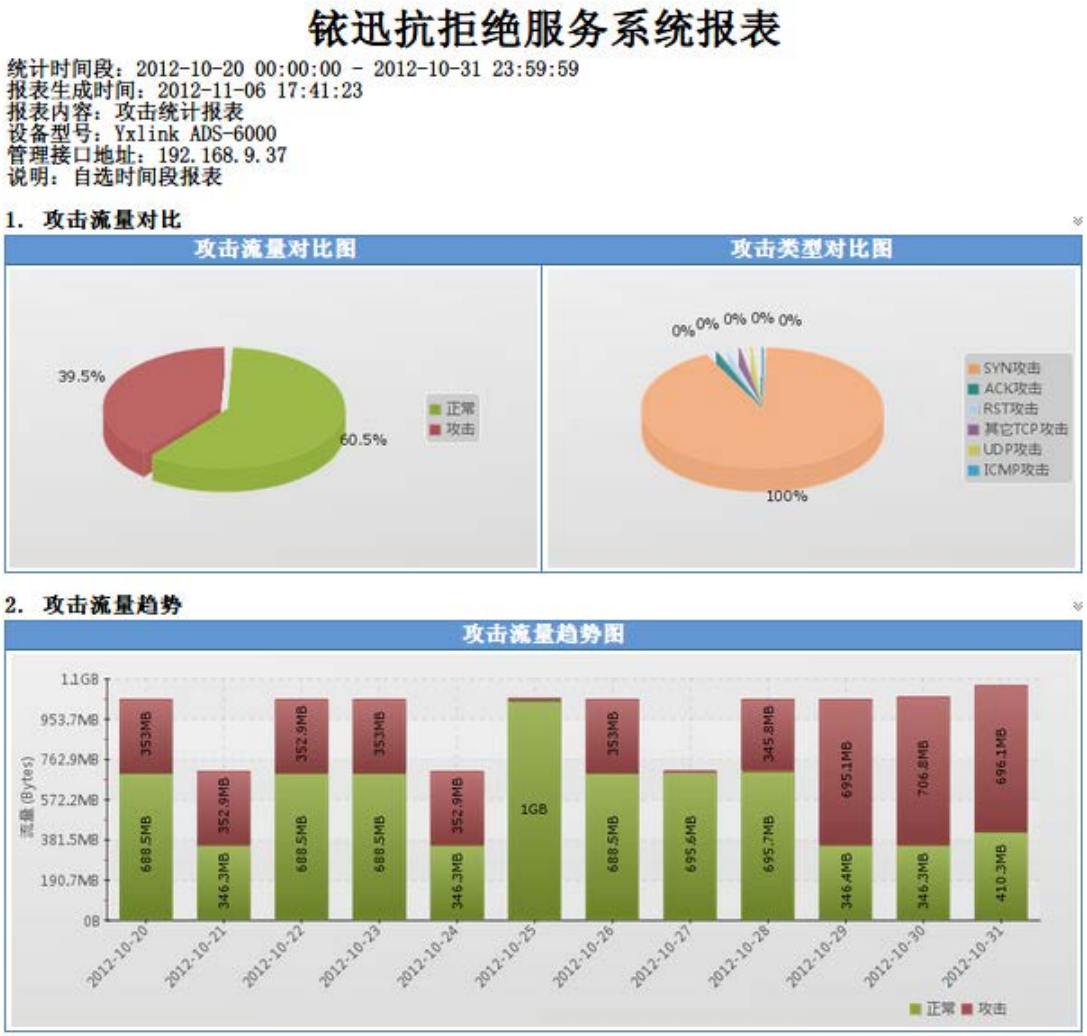
### 3.1.3 自定义过滤策略

自定义过滤作为铱迅抗拒绝服务系统的防御功能,为阻止新出现的攻击提供了有效手段。铱迅抗拒绝服务系统允许按照源、目的 IP 地址（或地址段），源/目的端口，协议类型，匹配规则，连接方向等方面自定义防御规则。

铱迅抗拒绝服务系统内置了若干预定义规则,理论上来说,任何具有数据包特征的攻击，都可以使用这个功能，自定义规则来防御。

### 3.1.4 统计报表

铱迅抗拒绝服务系统提供丰富详细的报表管理功能，可提供按指定日期生成 HTML、WORD2003、WORD2007 和 PDF 格式报表的功能。可以对生成的报表进行管理，能够按照设置自动生成报表并且发送至管理员邮箱。

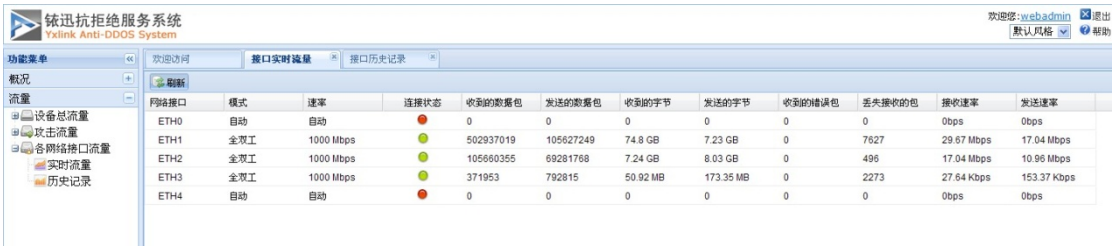



用户可设置自动生成报表的类型、时间、格式、是否邮件发送等配置信息，如果需要开启邮件发送的功能，需先配置好邮件通知。用户可以选择最近一个月，最近一周，当天，或者自定义统计范围，还可以为生成的报表填写相关说明信息。

## 3.2 产品优势

### 3.2.1 DDOS/DOS 流量自动建模拦截

铱迅抗拒绝服务系统可以通过对网络流量规律进行自动建模，从而深入识别隐藏在背景流量中的攻击报文，以实现精确的流量识别。




铱迅抗拒绝服务系统采用业界领先的“智能化流量模型”、“基于用户行为的单向防御”等技术，能够及时发现网络中的各种 DDOS 威胁并实现对攻击流量的快速过滤，从而有效保护城域网、IDC 等免遭海量 DDOS 攻击。在提供安全加固的同时，提升了带宽利用效率。

### 3.2.2 64 字节小包高性能处理

在实际网络环境中，64--256 字节的数据包最多，1000 字节以上次之，中间大小的数据包最少，也就是说小包数据处理能力才是衡量抗拒绝服务系统性能优劣的关键。64 字节小包是最小的网络数据包，从设备对网络数据的处理难度讲，对 64 字节小包的处理能力最能体现抗拒绝服务系统的真实性能。

黑客做 DDOS 攻击会利用小包来进行以达到快速耗费系统资源的目的，传统防御手段是利用防火墙所提供的阀值来限制，但使用这种方法阻抗网络攻击的能力有限，因为阀值只能限制数据包的数量，却不能限制数据包的大小。在整机吞吐能力有限的前提下，对小包 DDOS 攻击的抵御能力差，似乎成为防火墙的一个致命弱点。

铱迅抗拒绝服务系统产品的优越性恰恰体现在这里，在防御高达吞吐量 85%的 64 字节小包攻击时，系统表现依然良好，不仅延迟很少，且没有丢包现象，仍然能保证新建连接 100%的成功率，这是同类产品所不能比拟的。

### 3.2.3 灵活的部署能力

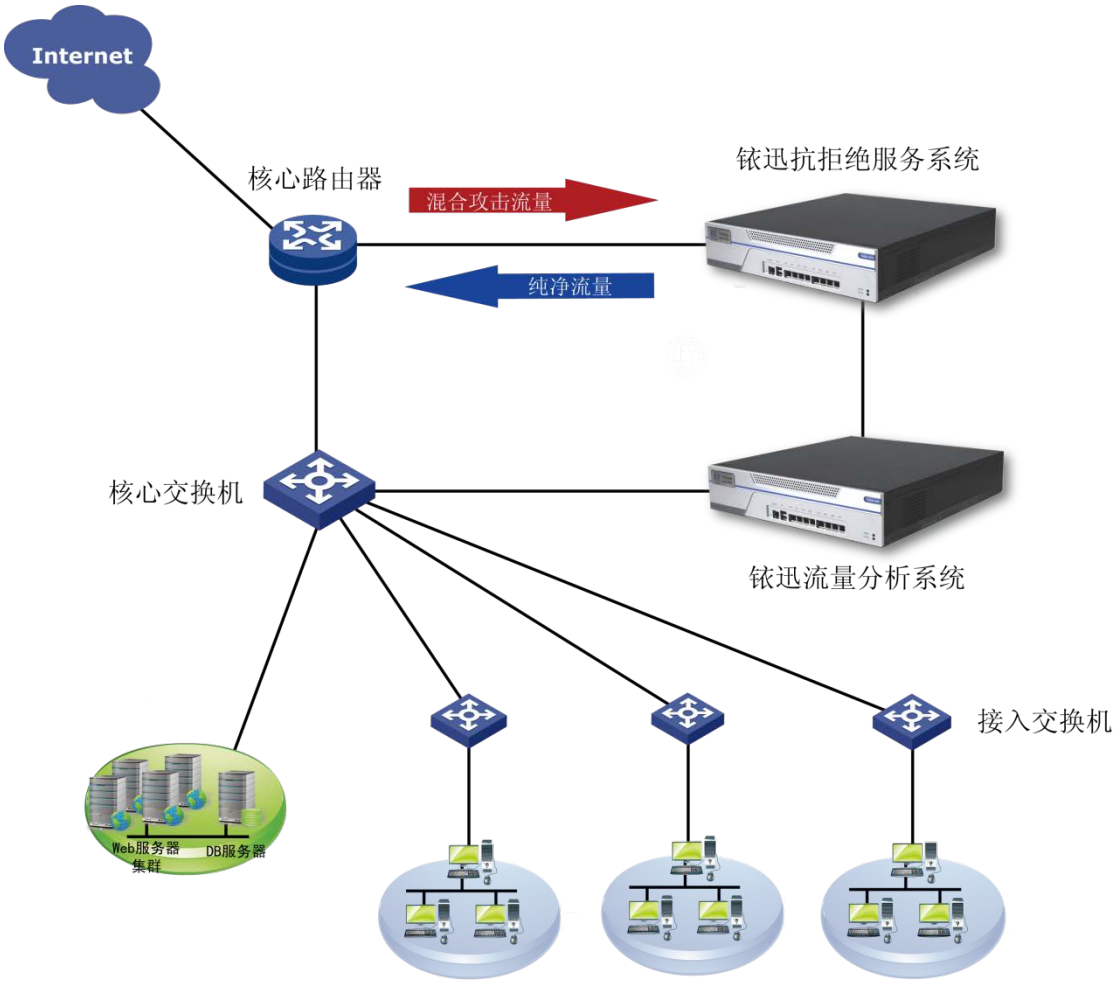
由于客户类型不同，抗拒绝服务所面临的网络环境也不同，企业网、IDC、ICP 或是城域网等多种网络协议并存，给抗拒绝服务系统的部署带来了不同的挑战。铱迅抗拒绝服务系统具备了多种环境下的部署能力，支持多种网络协议，诸如 BGP、VLAN 等，加之其基于应用的负载均衡能力，帮助整个产品成为多种客户环境下抗拒绝服务攻击的首选。

***串行部署方式：***

针对少量服务器或出口带宽较小的网络，铱迅抗拒绝服务系统提供串行部署方式，通过设备“串联”在网络入口端，对 DDOS 攻击进行检测、分析和阻断。

## *旁路部署方式：*

针对 IDC、ICP 或关键业务系统，铱迅抗拒绝服务系统提供了旁路部署的方式。通过设备中的流量监控功能，及时检测 DDOS 攻击的类型和来源。当发现 DDOS 攻击时，可启动流量牵引机制，从路由器或交换机处分流出可疑流量，完成 DDOS 攻击的过滤后，再将“干净”的流量注入网络中。

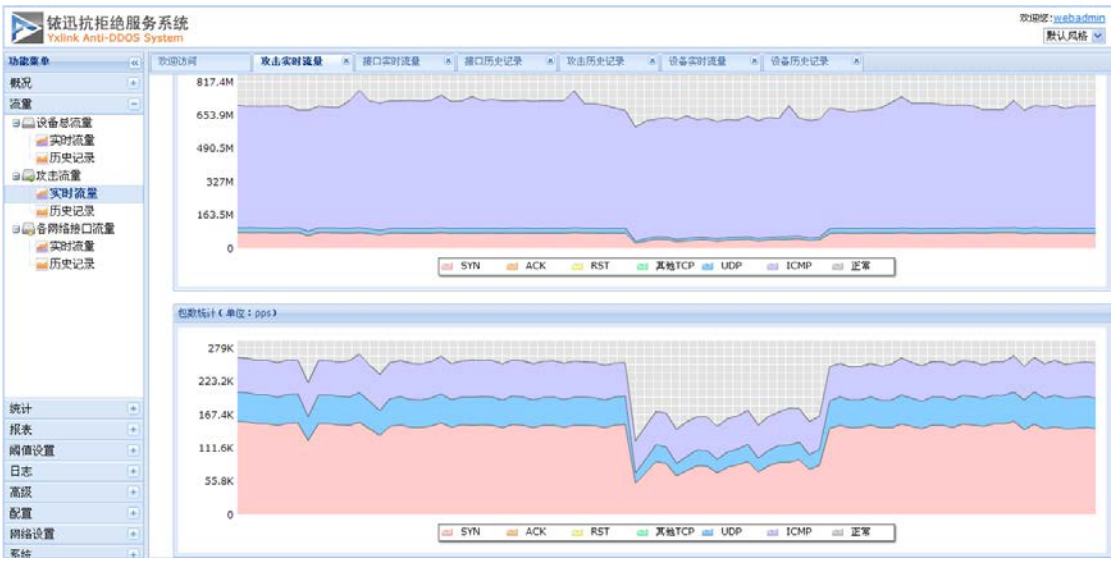


### 3.2.4 精准的实时流量监控

由于 DDOS 攻击越来越隐蔽，攻击的发起时刻到造成严重后果的时间间隔越来越短，因此以往的攻击侦测手段已经不适应当前网络安全管理中对网络攻击要“及时发现，快速定位，实时防范”的要求。

用统计的方法，可以在短时间内对大量数据进行处理，通过统计结果，可以及时准确的发现网络攻击，为准确定位和实施防范赢得了宝贵的时间。网络安全管理的重要原则是，侦测点离攻击的源头越近，侦测的效率越高。因此，“从源头阻断攻击”的方法成为防范 DOS/DDOS 攻击的最新理念，尤其是在对付分布式攻击的时候，从攻击源头的阻断是最有效的防护手段。

铱迅抗拒绝服务系统基于智能计算引擎的判断机制，可以通过监测实时流量，来发现未知的网络攻击。界面简单直观反映当前服务器流量信息、DDOS 攻击状态等，管理员通过实时流量图可以快速准确地掌握系统的运行状态。当受到 DDOS 攻击时，流量图示会出现明显的异常现象，管理员可以及时发现，并尽快处理。

# 四、结论

随着 DDOS 攻击工具不断的普遍和强大，Internet 上的安全隐患越来越多，以及客户业务系统对网络依赖程度的增高，可以预见的是 DDOS 攻击 事件数量会持续增长，而攻击规模也会更大，损失严重程度也会更高。由于这些攻击带来的损失增长，运营商、企业或是政府必须有所对策以保护其投资、利润和服务。

为了弥补目前安全设备（防火墙、入侵检测等）对 DDOS 攻击防护能力的不足，我们需要一种新的工具用于保护业务系统不受 DDOS 攻击的影响。这种工具不仅仅能够检测目前复杂的 DDOS 攻击，而且必须在不影响正常业务流量的前提下对攻击流量进行实时阻断。这类工具相对于目前常见的安全产品，必须具备更 细粒度的攻击检测和分析机制。

铱迅抗拒绝服务系统提供了业界领先的 DDOS 防护能力，通过多种机制的分析检测机制以及灵活的部署方式，能够有效的阻断攻击，保证合法流量的正常传输，这对于保障业务系统的运行连续性和完整性有着极为重要的意义。

# 铱迅信息

# *Yxlink*

南京铱迅信息技术有限公司

江苏省南京市雨花台区玉兰路86号智汇魔方206

销售与支持热线：400 097 5557

Nanjing Yxlink Information Technologies Co.,Ltd.

206 Cube of Wisdom, No. 86 Yulan Rd., Yuhua District, Nanjing, Jiangsu, China

**NJYXHADSWP012-11(01)**