产品概述

随着计算机网络信息化的快速发展， 越来越多的政府单位、金融机构和企业构建了自己的信息化系统，通过这些信息化系统，极大的提升了政府的办事效率，以及企业的管理和服务水平；然而这些信息化系统也面临着越来越多的网络攻击困扰，尤其是 DoS/DDoS 攻击的威胁。利用 DDoS 攻击手段敲诈勒索已经形成了一条完整的产业链！并且，攻击者实施成本极低，在网上可以随便搜索到一大堆攻击脚本、攻击工具，对攻击者的技术要求也越来越低。

DoS/DDoS（Denial of Service/Distributed Denial of Service），简称拒绝服务或分布式拒绝服务攻击。一直以来，它就是黑客实施点穴式攻击最有效的手段。DoS/DDoS 攻击者想方设法，使用各种网络技术手段，占用被攻击者所提供服务的资源，例如：消耗服务者的网络带宽资源、服务器的计算资源或者存储资源等等，让正常访问者无法获取相对应的资源，从而达到破坏的目的。

捷普异常流量清洗系统是专业的抗拒绝服务攻击产品，它能够从纷杂的网络背景流量中精准地识别出各种已知和未知的拒绝服务攻击流量，并能够实时过滤和清洗，确保网络正常访问流量通畅，是保障服务器数据可用性的安全产品。

产品特点

- 独特的连接代理防护算法

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 100%的新建连接的连接成功率。

- 高效的连接数据转发算法

抗拒绝服务系统系列产品，采用自主研发的 TCP 快速校验技术，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

抗拒绝服务系统系列产品，采用了基于 Linux 和 Windows 内插件技术，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

抗拒绝服务系统系列产品，采用基于页面插入式 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

抗拒绝服务系统系列产品，采用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 90%以上。

- 可扩展的集群模式

抗拒绝服务系统系列产品，采用可扩展的集群模式，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。

- 灵活多样的部署方式

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，如串联部署、双机热备部署、集群部署和旁路部署等。

产品功能

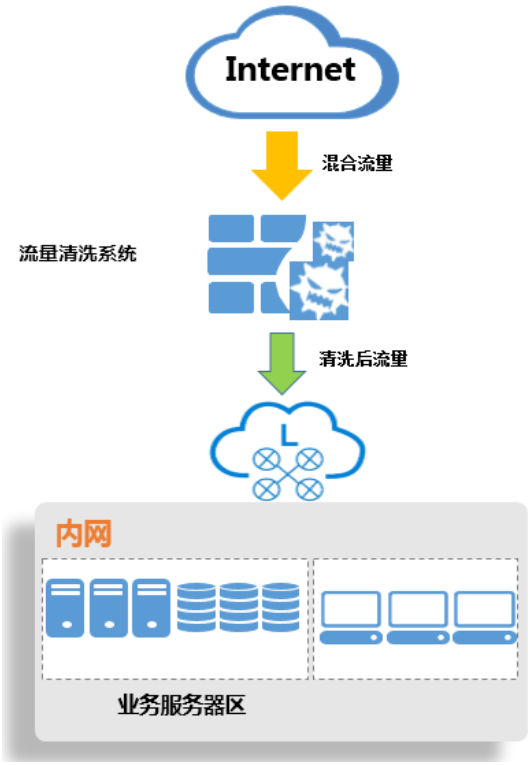
自主研发的抗拒绝服务攻击算法，拥有智能参数阀值，对 SYN Flood、UDP Flood、ICMP Flood、IGMP Flood、ACK Flood、DNS Query Flood、Ping Sweep 等流量型攻击，HTTP Proxy Flood、HTTP Get Flood、CC Proxy Flood、Connection Exhausted 等连接型攻击和 Smurf、Land-based、Teardrop、Fragment Flood、Red Code 等漏洞型攻击及其他各种常见的攻击行为均可有效识别，并通过集成的机制实时对这些攻击流量进行阻断处理，保障业务系统正常运行。内置的各种针对网站、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 DoS 攻击。

产品部署

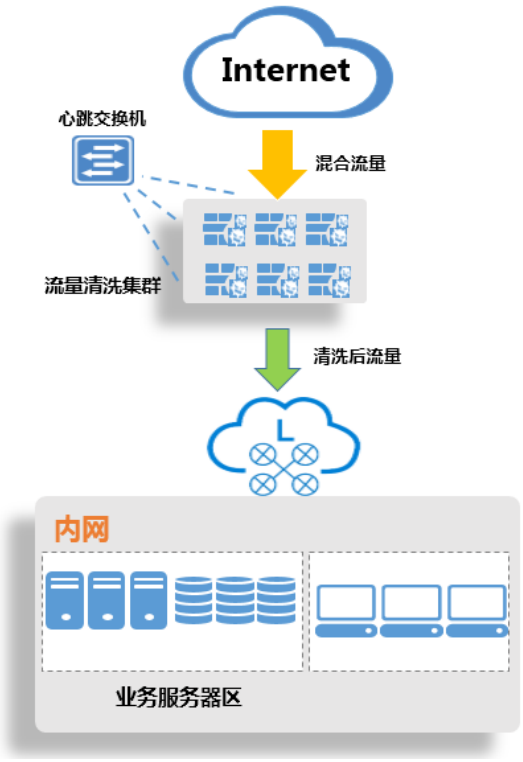
捷普异常流量清洗系统有两种最基本的部署方式：串行透明部署和旁路部署，且支持集群部署。

串行透明部署方式

串联透明模式部署简单，网络隐身，无 IP 地址配置,不需要改变网络中的路由走向。串行透明部署支持单机部署的同时也支持集群部署。



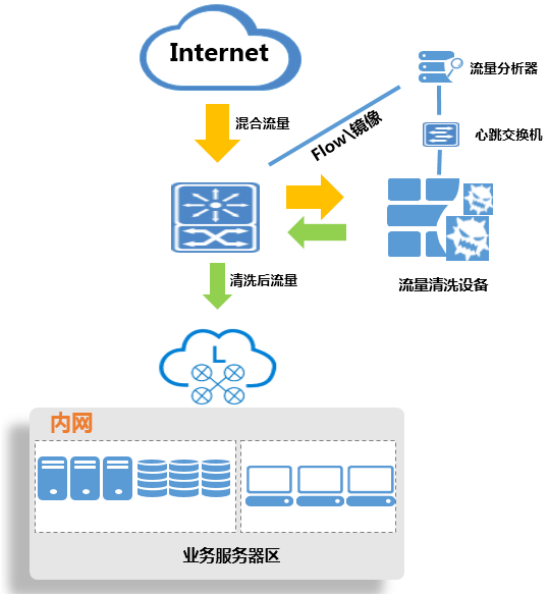
串行透明单独部署



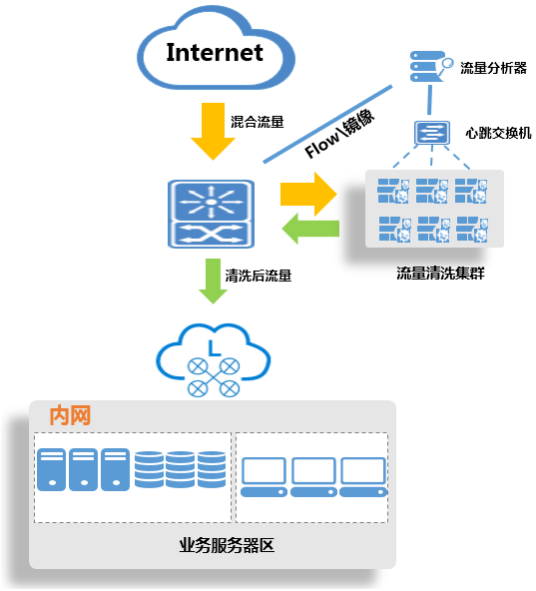
串行透明集群部署

旁路部署方式

和串联部署相比，旁路部署通常都要增加一台流量分析设备，分析设备通过与清洗设备相连的心跳线发送清洗通知牵引某受保护的 IP 流量， 清洗设备向其邻接关系发送此 IP 的主机路由宣告，此时路由器更新路由表，并把主机的路由已经指向清洗设备接口，之后的关于此主机 IP 的所有的流量都会直接转发至清洗设备，清洗设备对流量进行检测、准确地拦截异常流量后，最后将过滤后的纯净流量再次通过注入或回注的方式将纯净的流量转发到网络中去。 当清洗设备发现某主机 IP 流量已经正常了，清洗设备向路由器发送取消此 IP 的主机路由宣告，此时 IP 的流量又重新按原来的网络路径转发到目的网络，旁路部署配置相对复杂，但系统网络不发生变化，没有单点故障。


Internet
流量分析器
混合流量
Flow镜像
心跳交换机
清洗后流量
流量清洗设备
内网
业务服务器区

旁路部署


Internet
流量分析器
混合流量
Flow镜像
心跳交换机
清洗后流量
流量清洗集群
内网
业务服务器区

旁路集群部署