



中新金盾抗拒绝服务系统 技术白皮书

版本号：201102A

文档信息

版权声明

本文件所有内容受版权保护并且归中新软件所有。未经中新软件明确书面许可，不得以任何形式复制、传播本文件（全部或部分）。

中新软件、GFW、金盾抗拒绝服务系统是安徽中新软件有限公司注册商标，本文中涉及到的其它产品名称和品牌为其相关公司或组织的商标或注册商标，特此鸣谢。

本文件仅供技术学习参考，安徽中新软件不对本文件的内容及使用负任何责任或保证。另外，安徽中新软件对本文件保留修改权利。

目 录

概述	4
产品概况	5
金盾 GFW-7050	5
金盾 GFW-7100	6
金盾 GFW-7200	7
金盾 GFW-7400	8
金盾 GFW-7180	9
金盾 GFW-7700	10
产品技术规范和标准	11
金盾抗拒绝服务系统技术创新	12
金盾抗拒绝服务系统防护功能介绍	13
产品功能	13
防护原理	14
部署方式	16
单机串联	16
双机热备	17
串联集群	19
旁路（回流模式）	20
旁路（注入模式）	21

概述

拒绝服务攻击（DOS/DDOS）是近年来愈演愈烈的一种攻击手段，其主要目的是造成目标主机的 TCP/IP 协议层拥塞、或者导致应用层异常终止而形成拒绝服务现象。目前，DOS/DDOS 攻击方式主要有以下几种：

- ◆ 利用 TCP/IP 协议的漏洞，消耗目标主机的系统资源，使其过度负载。此种攻击也是目前最普遍存在的一种攻击形式，攻击者动辄发起几十兆甚至上百兆的攻击流量，造成目标的彻底瘫痪。常见的有 SYN Flood，UDP Flood，ICMP Flood 等等；
- ◆ 利用某些基于 TCP/IP 协议的软件漏洞，造成应用异常。此种攻击比较单一，通常是针对某个软件的特定版本的攻击，影响范围较小，且具有时限性。但通常此种攻击较难防治，漏洞查找较困难；
- ◆ 不断尝试，频繁连接的野蛮型攻击。此种攻击早期危害有限，但随着代理型攻击的加入，已渐有成为主流之势。常见的有 web stress，CC Proxy Flood 等。

随着网络上各种业务的普遍展开，DOS/DDOS 攻击所带来的损失也愈益严重。当前运营商、企业及政府机构的各种用户时刻都面临着攻击的威胁，而可预期的更加强大的攻击工具也会成批出现，此种攻击只会数量更多、破坏力更强大，更加难以防御。

正是 DOS/DDOS 攻击难于防御，危害严重，所以如何有效的应对 DOS/DDOS 攻击就成为对网络安全工作者的严峻挑战。传统网络设备或者边界安全设备，诸如抗拒绝服务系统、入侵检测系统，作为整体安全策略中不可缺少的重要模块，都不能有效的提供针对 DOS/DDOS 攻击完善的防御能力。因此必须采用专门的机制，对攻击进行检测、防护、进而遏制这类不断增长的、复杂的且极具隐蔽性的攻击形为。

产品概况

金盾抗拒绝服务系统针对基于 Internet 的信息平台，需要对不可控网络提供实时服务的客户，为其提供完善的安全防护措施，使其免受恶意攻击的危害

金盾抗拒绝服务系统应用了自主研发的抗拒绝服务攻击算法，对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处理及阻断，保护服务主机免于攻击所造成的损失。

金盾 GFW-7050



金盾 GFW-7050

详细参数

外形	1U 机架式		
级别	百兆级		
网络接口	4 个 10/100/1000M 以太网电口		
吞吐量	500M		
抗攻击性能	64 字节	128 字节	256 字节
	500Mbps	500Mbps	500Mbps
说明	适合百兆、千兆电口环境, 工商, 税务, 社保, 医疗及网吧等小中型企业。		
特性	各种DDOS攻击防护/应用层协议及端口保护/特殊应用的保护/流量监控/数据包规则过滤/数据包捕获分析/攻击日志记录、审计报告/网络隐身、透明接入/旁路/集群防护等		
防御种类	可对Smurf、Land-based、Teardrop、PingSweep、IP Spoof、Code Red、IP Fragmentation Overlap、SYN Flood、ACK Flood、UDP Flood、DNS Query Flood、ICMP Flood、PING of Death、PING Flood、IGMP Flood、Fragment Flood、HTTP Get Flood、HTTP Proxy Flood、CC Proxy Flood 等各种常见的攻击流量有效识别和过滤		
电源	交流电源输入 100V~220V, 47~63MHZ, <180W		
工作温度	-20℃--60℃		
MTBF	>120000 小时		

金盾 GFW-7100



金盾 GFW-7100

详细参数

外形	2U 机架式		
级别	千兆（入门级）		
网络接口	2 个 1000M SFP 接口插槽(可选配模块)，5 个 100/1000M 以太网电口		
吞吐量	1G		
抗攻击性能	64 字节	128 字节	256 字节
	0.85Gbps	1Gbps	1Gbps
说明	适合千兆环境（ 单多模环境、光电口环境可选 ）适合中型企业，政府、军事、教育，交通等		
特性	各种DDOS攻击防护/应用层协议及端口保护/特殊应用的保护/流量监控/数据包规则过滤/数据包捕获分析/攻击日志记录、审计报告/网络隐身、透明接入/旁路/集群防护等		
防御种类	可对Smurf、Land-based、Teardrop、PingSweep、IP Spoof、Code Red、IP Fragmentation Overlap、SYN Flood、ACK Flood、UDP Flood、DNS Query Flood、ICMP Flood、PING of Death、PING Flood、IGMP Flood、Fragment Flood、HTTP Get Flood、HTTP Proxy Flood、CC Proxy Flood 等各种常见的攻击流量有效识别和过滤		
电源	交流电源输入 100V~220V，47~63MHZ，<510W（可扩展至双电源）		
工作温度	-20℃--60℃		
MTBF	>120000 小时		

金盾 GFW-7200



金盾 GFW-7200

详细参数

外形	2U 机架式		
级别	千兆（企业级）		
网络接口	4 个 1000M SFP 接口插槽(可选配模块)，4 个 100/1000M 以太网电口		
吞吐量	2G		
抗攻击性能	64 字节	128 字节	256 字节
	1.7Gbps	2Gbps	2Gbps
说明	适合多路接入环境（ 单多模环境可选 ）适用于双千 M 接入环境，政府、军事、教育、金融、电力、工商、税务、社保、公安、烟草、外贸、医疗等		
特性	各种DDOS攻击防护/应用层协议及端口保护/特殊应用的保护/流量监控/数据包规则过滤/数据包捕获分析/攻击日志记录、审计报告/网络隐身、透明接入/旁路/集群防护等		
防御种类	可对Smurf、Land-based、Teardrop、PingSweep、IP Spoof、Code Red、IP Fragmentation Overlap、SYN Flood、ACK Flood、UDP Flood、DNS Query Flood、ICMP Flood、PING of Death、PING Flood、IGMP Flood、Fragment Flood、HTTP GetFlood、HTTP Proxy Flood、CC Proxy Flood等各种常见的攻击流量有效识别和过滤		
电源	交流电源输入 100V~220V，47~63MHZ，<510W（ 可扩展至双电源 ）		
工作温度	-20℃--60℃		
MTBF	>120000 小时		

金盾 GFW-7400



金盾 GFW-7400

详细参数

外形	2U 机架式		
级别	千兆（电信级）		
网络接口	8 个 SFP 接口(进出口, 可选配模块), 2 个千 M 电口(管理口) 集群接口可选		
吞吐量	4G		
抗攻击性能	64 字节	128 字节	256 字节
	3.4Gbps	4Gbps	4Gbps
说明	适合多路接入环境（ 单多模环境可选 ）适用于 4 路千 M 接入环境，政府、军事、教育、金融、电力、工商、税务、社保、公安、烟草、外贸、医疗等		
特性	各种DDOS攻击防护/应用层协议及端口保护/特殊应用的保护/流量监控/数据包规则过滤/数据包捕获分析/攻击日志记录、审计报告/网络隐身、透明接入/旁路/集群防护等		
防御种类	可对Smurf、Land-based、Teardrop、PingSweep、IP Spoof、Code Red、IP Fragmentation Overlap、SYN Flood、ACK Flood、UDP Flood、DNS Query Flood、ICMP Flood、PING of Death、PING Flood、IGMP Flood、Fragment Flood、HTTP GetFlood、HTTP Proxy Flood、CC Proxy Flood等各种常见的攻击流量有效识别和过滤		
电源	交流电源输入 100V~220V, 47~63MHZ, <510W（ 可扩展至双电源 ）		
工作温度	-20℃--60℃		
MTBF	>120000 小时		

金盾 GFW-7180



金盾 GFW-7180

详细参数

外形	2U 机架式		
级别	千兆（入门级）		
网络接口	2 个 1000M SFP 光纤接口(支持 Bypass 功能)，2 个 100/1000M 以太网电口		
吞吐量	1G		
抗攻击性能	64 字节	128 字节	256 字节
	0.85Gbps	1Gbps	1Gbps
说明	适合单千 M 接入环境，适用于政府、军事、教育、金融、电力、工商、税务、社保、公安、烟草、外贸、医疗、运营商等对网络稳定性要求较高的网络		
特性	各种DDOS 攻击防护/应用层协议及端口保护/特殊应用的保护/流量监控/数据包规则过滤/数据包捕获分析/ 攻击日志记录、审计报告/ 网络隐身、透明接入/ 旁路/ 集群防护等/ 支持Bypass功能（系统崩溃，硬件故障，意外断电等情况下也不会中断网络）		
防御种类	可对Smurf、Land-based、Teardrop、PingSweep、IP Spoof、Code Red、IP Fragmentation Overlap、SYN Flood、ACK Flood、UDP Flood、DNS Query Flood、ICMP Flood、PING of Death、PING Flood、IGMP Flood、Fragment Flood、HTTP GetFlood、HTTP Proxy Flood、CC Proxy Flood等各种常见的攻击流量有效识别和过滤		
电源	交流电源输入 100V~220V，47~63MHZ，<700W（双冗余电源）		
工作温度	-20℃--60℃		
MTBF	>120000 小时		

金盾 GFW-7700



金盾 GFW-7700

详细参数

外形	4U 机架式		
级别	万兆级		
网络接口	2 个 10000M SFP+ 光纤接口, 2 个 1000M SFP 接口插槽 (可选配模块), 2 个 100/1000M 以太网电口		
吞吐量	10G		
抗攻击性能	64 字节	128 字节	256 字节
	10Gbps	10Gbps	10Gbps
说明	适合万 M 接入环境, 适用于运营商、政府、军事、教育、金融、电力、工商、税务、社保、公安、烟草、外贸、医疗、能源系统等。		
特性	各种DDOS攻击防护/应用层协议及端口保护/特殊应用的保护/流量监控/数据包规则过滤/数据包捕获分析/攻击日志记录、审计报告/网络隐身、透明接入/旁路/集群防护等		
防御种类	可对Smurf、Land-based、Teardrop、PingSweep、IP Spoof、Code Red、IP Fragmentation Overlap、SYN Flood、ACK Flood、UDP Flood、DNS Query Flood、ICMP Flood、PING of Death、PING Flood、IGMP Flood、Fragment Flood、HTTP GetFlood、HTTP Proxy Flood、CC Proxy Flood等各种常见的攻击流量有效识别和过滤		
电源	交流电源输入 100V~220V, 47~63MHZ, <764W (双冗余电源)		
工作温度	-20℃--60℃		
MTBF	>120000 小时		

说明：以上图片为金盾抗拒绝服务系列抗拒绝服务系统，产品均为实物拍摄

产品技术规范 and 标准

- ◆ 网桥。工作于 ISO 的 OSI7 层参考模型中的第二层数据链路层的 MAC 子层，通过转发 MAC 帧实现网络互联。符合 ANSI/IEEE Std 802.1D
 - ◆ 支持虚拟局域网 VLAN 。符合 ANSI/IEEE Std 802.1Q
 - ◆ 支持点对点协议 PPPoE 。符合 RFC 2516
 - ◆ 支持 ARP/RARP 协议，符合 RFC826 。并可根据 ARP 通信自动识别受保护主机
 - ◆ 支持 IPv4 协议，符合 RFC791 。并可根据 IP 通信量自动识别受保护主机
 - ◆ 支持 TCP/UDP/ICMP 等协议，符合 RFC793/768/792 等。
 - ◆ 支持规则过滤模式，具有包检测型抗拒绝服务系统功能。同时还支持关键字过滤、正则表达式匹配等深层过滤模式
 - ◆ 支持基于 IP 的流量控制模式，限制某主机的流量 具有基于 802.3ad 链路聚合实现的集群模式，形成多点处理，避免单点故障
-
- 对于 TCP 协议，通过 SYN Proxy ， 延时重传，连接跟踪等技术，完成 DOS/DDOS 的攻击防御。 并具有可扩充的插件模式用于应用层防御模式。
 - 对于 UDP 协议，通过同步连接，延时重传，连接跟踪等技术，完成 DOS/DDOS 的攻击防御。并具 有可扩充的插件模式用于应用层防御模式。
 - 对于 ICMP 及其它协议，主要通过流量限制方式完成 DOS/DDOS 的攻击防御。

金盾抗拒绝服务系统技术创新

连接代理防护模式—— SYN Proxy 以代理模式处理客户端和服务器之间的连接，同时完成攻击报文的过滤。即使在海量攻击下仍可保证 100% 的新建连接成功率；

连接数据转发算法—— TCP Fast Rechecksum 高效的处理 TCP 连接数据及其校验和，而无需重新统计报文数据；

内核防护插件—— Kernel Protection Plugin, for Linux&Windows 将特定防护算法以模块形式实现，简化核心代码，优化系统构架，并且具有良好的扩展性；

页面插入式 Web 防护算法—— Web Protection based on Page Injection 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，达到高效防御 Web 类连接攻击的目的；

数据挖掘式通用防护算法—— Generic Protection based on Data Mining 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，有效率达到 90% 以上；

可扩展的集群模式—— Extensible Firewall Cluster Mode 领先的数据分流技术，使得若干抗拒绝服务系统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；

内核防盗版技术—— Anti-Cracking Mechanism in Kernel 实现在系统核心的加密技术，使得本系统具有较强的防盗版、防拷贝能力；

多平台构架支持—— Multiple Platform & Architecture Support 基于 Windows NDIS 的软件产品，支持 x86 ， AMD64 ， IA64 构架；基于 Linux 的硬件产品，百兆型、千兆型及集群型多种解决方案。

金盾抗拒绝服务系统防护功能介绍

针对当前的 DOS/DDOS 攻击现状，安徽中新软件自主研发的抗拒绝服务产品——金盾抗拒绝服务系统，具有很强的 DOS/DDOS 攻击的防护能力。并可在多种网络环境下轻松部署，保证网络的整体性能和可靠性。

产品功能

◆ DOS/DDOS 攻击检测及防护

金盾抗拒绝服务系列产品，应用了自主研发的抗拒绝服务攻击算法，对 SYN Flood, UDP Flood, ICMP Flood, IGMP Flood, Fragment Flood, HTTP Proxy Flood, CC Proxy Flood, Connection Exhausted 等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处理及阻断，保护服务主机免于攻击所造成的损失。内建的 WEB 保护模式及游戏保护模式，彻底解决针对此两种应用的 DOS 攻击方式。

◆ 通用方便的报文规则过滤

金盾抗拒绝服务系列产品，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，可设置的域包括地址、端口、标志位，关键字等，极大的提高了通用性及防护力度。同时，内置了若干预定义规则，涉及局域网防护、漏洞检测等多项功能，易于使用。

◆ 专业的连接跟踪机制

金盾抗拒绝服务系列产品，内部实现了完整的 TCP/IP 协议栈，具有强大的连接跟踪能力。每个进出的连接，抗拒绝服务系统都会根据其源地址进行分类，并显示给用户，方便用户对受保护主机状态的监控。同时还提供连接超时，重置连接等辅助功能，弥补了 TCP 协议本身的不足，使您的服务器在攻击中游刃有余。

◆ 简洁丰富的管理

金盾抗拒绝服务系列产品具有丰富的设备管理功能，基于简洁的 WEB 的管理方式，支持本地或远程的升级。同时，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。

◆ 广泛的部署能力

针对不同的客户，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。金盾抗拒绝服务系统具备了多种环境下的部署能力。

防护原理

金盾抗拒绝服务产品基于嵌入式系统设计，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。并采用自主研发的高效的防护算法，效率极高。方案的核心技术架构如下图所示：



➤ **主机识别**

金盾抗拒绝服务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**

金盾抗拒绝服务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**

攻击过滤为抗拒绝服务系统的默认模式，此模式下，抗拒绝服务系统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。当某数据包的原 MAC 地址不同于抗拒绝服务系统记录到的 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。

- 端口保护

建立在连接跟踪模块上的端口防护体制，针对不同的 TCP/UDP 端口应用，提供不同的防护手段，使得运行在同一服务器上的不同服务，都可以受到完善的 DOS/DDOS 攻击保护。

- 连接控制

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

- 连接跟踪

金盾抗拒绝服务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。

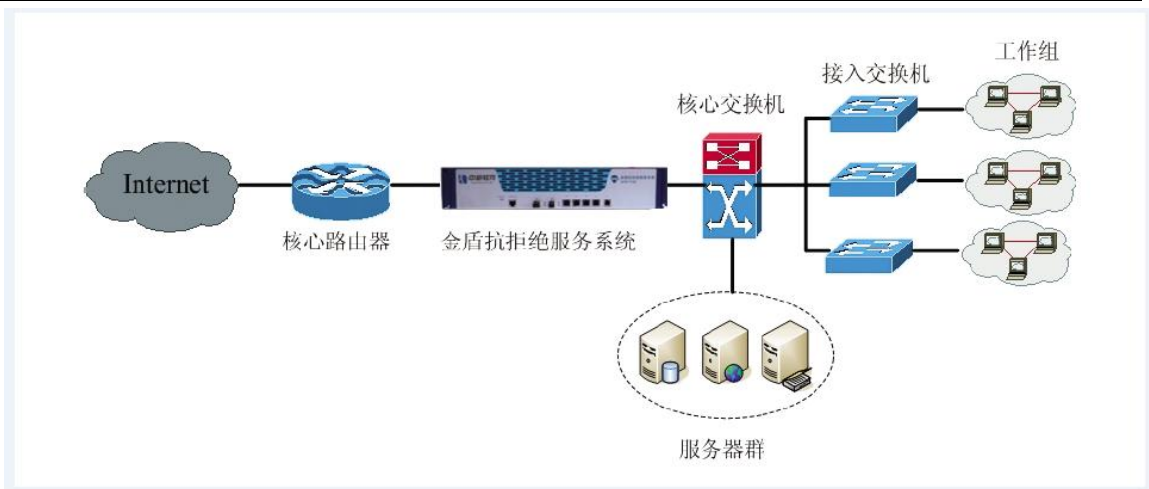
- 日志审计

抗拒绝服务系统日志记录可全面记录产品系统运行及防护状态，并对不同操作权限的操作进行记录。

部署方式

金盾抗拒绝服务系统采用透明模式和旁路模式接入，符合目前大多数网络结构防护需求，根据客户不同的需求，设定合适的部署方式。

单机串联

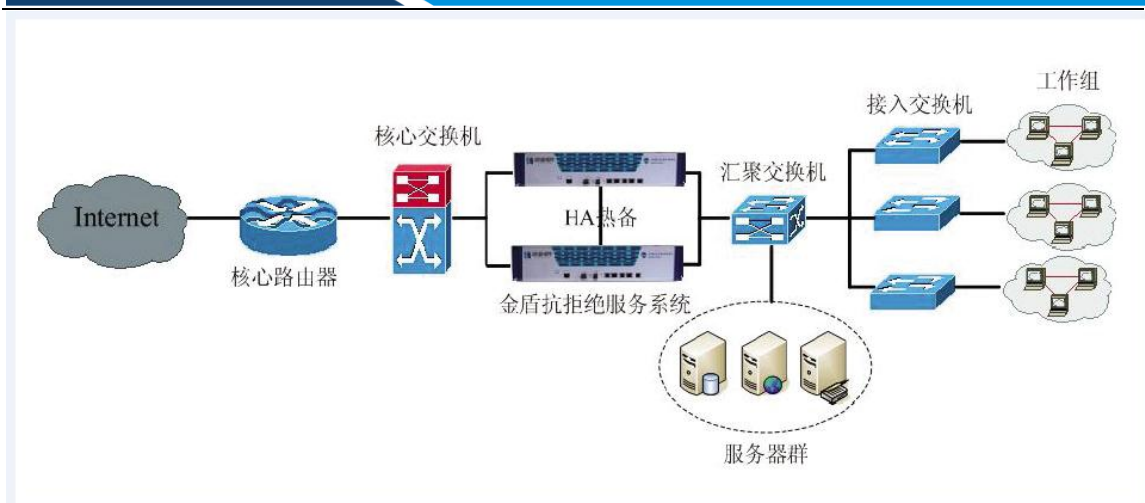


金盾抗拒绝服务系统接入机房核心交换机前端防护，核心交换机下所有主机进入防护区，连接方式：将 ISP（运营商）分配的光纤接入到金盾抗拒绝服务系统设备进口，再将金盾抗拒绝服务系统设备出口接到下层核心交换机，被保护主机可置于核心交换机下。

安装步骤如下：

- 连接数据端口，将外网连接线（数据入线）接入抗拒绝服务系统上标识为“进口”的网口，相应的内网连接线（数据出线）接入抗拒绝服务系统上标识为“出口”的网口；
- 连接管理接口，将抗拒绝服务系统的任一标识为“管理口”的网口接入外网或内网交换机；
- 启动抗拒绝服务系统，连接电源线并启动电源开关，检查接线的各个网口的指示灯是否正常闪烁；
- 登陆管理机，更改 IP 地址为与抗拒绝服务系统管理地址同一网段，随后登陆管理界面，确保可以正常访问；
- 查看流量，确认数据正常通行，完成安装。

双机热备



金盾抗拒绝服务系统为了保证网络的高可用性与高可靠性，抗拒绝服务系统提供了双机热备份功能，即在同一个网络节点使用两个配置相同的抗拒绝服务系统。双机热备模式采用两种工作模式，主—主模式和主—从模式，两种模式详细介绍：

主—主：工作模式即让两台抗拒绝服务系统同时工作，当任意服务器发生故障，如接口及连线故障、意外 down 机、关键进程失败、性能下降、CPU 和内存负载过大等情况，另一台抗拒绝服务系统能够平滑的接替该抗拒绝服务系统的工作，并保持连接，实现负载均衡。

主—从：正常情况下主抗拒绝服务系统处于工作状态，另一个抗拒绝服务系统处于备份状态，称为从抗拒绝服务系统。当主抗拒绝服务系统发生意外 down 机、网络链路发生故障、硬件故障等情况时，从抗拒绝服务系统自动进行切换工作状态，从抗拒绝服务系统代替主抗拒绝服务系统正常工作，从而保证了网络的正常使用。

切换过程不需要人为操作和其他系统的参与，切换时间控制在 10 秒以内。

抗拒绝服务系统软件系统设置

在双机热备的系统中，两台抗拒绝服务系统的软件版本必须相同，网络口的数目和类型也要相同；两台产品可以实现同步操作。

抗拒绝服务系统管理 “集群页面” 详细设置如下

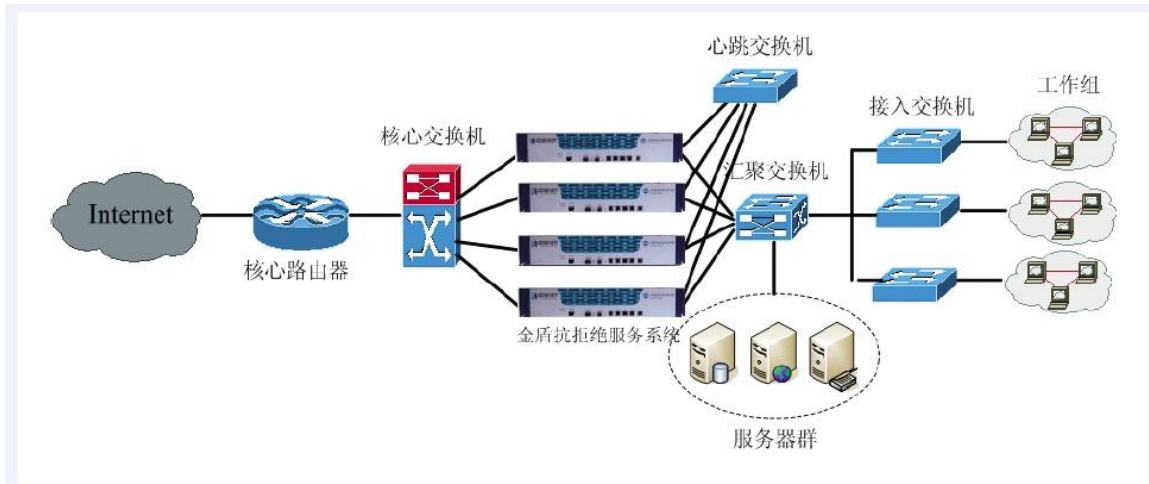
热备设置方式：要先设置集群地址；

设置热备模式：在主设备上设置激活模式，备设备上设置备份模式。多路激活不要选。（后期扩展用）；

异常切换时间：可以任意填写，单位为 XX 秒；

链路检测地址：可以设 4 个，包括设备内和设备外的地址，（所设置的地址和设备的管理地址之间的数据跨过抗拒绝服务系统）抗拒绝服务系统每秒会 ping 所设置的地址，从而来探测流量是否异常，如出现异常中断抗拒绝服务系统则自动将数据切换到备用线路。

串联集群



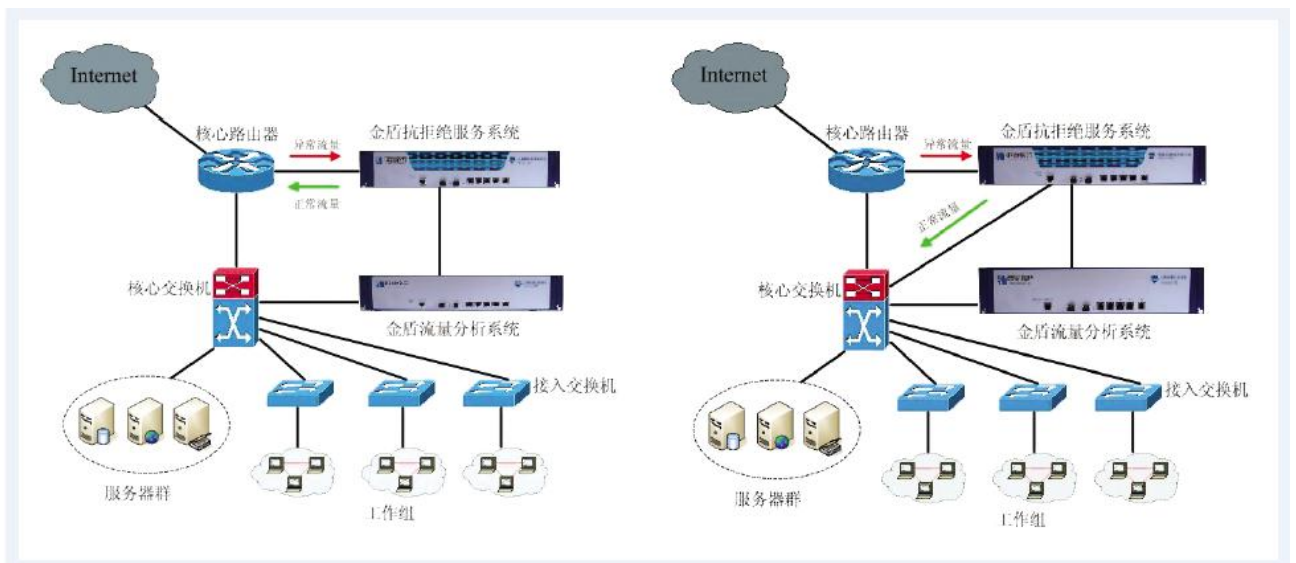
集群型抗拒绝服务系统依靠多台抗拒绝服务系统实现防护带宽及防护能力的叠加，目前可支持多台抗拒绝服务系统形成集群，抵御大的攻击流量。首先在交换机的相应端口设置端口聚合——Port Trunking（某些交换机称为链路聚合——Link Aggregation），或者直接设置路由器完成线路的聚合，分别接入抗拒绝服务系统，每个抗拒绝服务系统接入一路数据（入口和出口）。

集群型抗拒绝服务系统安装步骤如下：

- a) 重新设置抗拒绝服务系统地址，规划集群抗拒绝服务系统的序号，随后依次开启抗拒绝服务系统，连接管理口，配置抗拒绝服务系统的IP地址，将抗拒绝服务系统所有网卡的地址改为与其序号相对应，这样就可以避免集群中的抗拒绝服务系统出现IP地址冲突的情况；
- b) 连接数据端口，依次将每条线路的外网连接线（数据入线）接入抗拒绝服务系统上标识为“进口”的网口，相应的内网连接线（数据出线）接入抗拒绝服务系统上标识为“出口”的网口；
- c) 连接心跳线路，依次将每台抗拒绝服务系统的心跳口接入交换机（千兆型集群需接入千兆型交换机）。如果是两台抗拒绝服务系统形成的集群，则心跳线路可直接利用交叉线对接；
- d) 连接管理接口，依次将每台抗拒绝服务系统的任一标识为“管理口”的网口接入内网交换机；
- e) 在外部交换机上，将数据入口设置为端口聚合。在内部交换机上同样将数据出口设置为端口聚合；

- f) 登陆管理机，更改 IP 地址为与抗拒绝服务系统管理地址同一网段，随后登陆管理界面，进入集群设置页面，输入抗拒绝服务系统 ID 所对应的心跳口的 IP 地址，随后保存；
- g) 注意，启动抗拒绝服务系统后集群功能自动生效；
- h) 查看流量，确认数据正常通行，完成安装。

旁路



旁路（回流模式上图（左））

回流模式，抗拒绝服务系统在处理过流量之后，将纯净流量再次从原路发回网络。该模式下，需要在核心路由器上配置策略路由，将从抗拒绝服务系统发回的流量直接送至下层设备，否则核心路由器和抗拒绝服务系统之间会形成流量的无限循环。

中新软件推出的抗拒绝服务旁路系统由金盾抗拒绝服务系统和金盾流量分析器组成：

金盾抗拒绝服务系统：

对攻击流量、异常、潜在攻击流量进行彻底检测,去除攻击流量等,转发过滤后的干净流量。

金盾流量分析器：

对网络流量进行分析，将与受保护 IP 有关的异常流量信息通知金盾抗拒绝服务系统。

旁路（注入模式上图（右））

注入模式，抗拒绝服务系统处理流量之后，将纯净流量直接注入下层设备。采用此种模式，考虑下层设备的不同，有两种不同配置：

- 若下层设备为交换机，则抗拒绝服务系统将自动解析目标主机的 MAC 地址，并将纯净流量直接发送至该主机；
- 若下层设备为路由器，则需要在抗拒绝服务系统上设置下层路由器的地址（下一跳地址）若是集群则每台设备都要独立设置。

分析器（Analyzer）

分析器用于从用户网络中识别出攻击行为，并通知抗拒绝服务系统进行牵引处理，同时还收集一些连接信息提供给抗拒绝服务系统，因此分析器目前只支持镜像/分光

（Mirror/SPAN）模式。分析器接入核心路由器的下层，以便在遇到大流量攻击的情况下，分析器的端口不被攻击流量完全堵塞。

抗拒绝服务系统（Protector）

抗拒绝服务系统设备在网络流量正常情况下，处于非激活状态。当分析器识别出攻击流量后，通知抗拒绝服务系统设备，随后防护设备通过 BGP 路由通告，从核心路由器将流量牵引到抗拒绝服务系统进行处理，并将过滤后的流量重新提交到原网络。

安徽中新软件有限公司

网 址：www.cnzxsoft.com

24 小时技术支持热线：800-868-7722

售后服务直线：86-0551-5321158、5321558