H3C SecPath AFC2000 异常流量清洗

产品概述

DDoS 防护服务市场领导者 Black Lotus 发布的最新报告显示，全球大型服务提供商都饱受各种 DDoS 攻击。攻击范围非常广泛，涵盖各行各业，其中 64%的平台提供商受到 DDoS 攻击影响，66%的托管解决方案提供商和 66%的 VoIP 服务提供商受到影响。

DDoS 攻击会造成非常严重的影响，61%的各类型服务提供商因被攻击而威胁到正常的商业运作，甚至造成利润流失或者客户隐私被窃。越来越多信息系统维护方对防范拒绝服务攻击日益重视，已成为系统信息安全保障的重要要求之一，抗拒绝服务系统产品也应运而生，新华三技术有限公司投入大量人力和资金研发出了异常流量清洗系统。

新华三异常流量清洗产品基于嵌入式系统设计，其核心采用自主研发的高效防护算法，创造性的将算法实现在协议栈最底层，使整个运算代价大大降低。同时，产品采用全新一代多核处理器硬件平台，整机采用主动探测防护，全系列型号产品均达到 64 字节小包线速，整机性能更高。产品主要用于抵抗拒绝服务类的网络攻击，例如：SYN-flood、UDP-flood、DNS-Query-flood 等类型攻击，产品旨在应用于 IDC 机房，政府、事业单位，大型企业，为客户解决拒绝服务类的攻击防护问题，保证重要网络环境的安全和完整性，创造安全可靠的网络环境。

图1-1 H3C SecPath AFC2020 产品外观图

图1-2 H3C SecPath AFC2040 产品外观图

图1-3 H3C SecPath AFC2100 产品外观图

图1-4 H3C SecPath AFC2100-D 产品外观图

图1-5 H3C SecPath AFC2200 产品外观图

产品特点

精确智能的攻击检测及防护

- 拥有自主的抗拒绝服务攻击算法，拥有智能参数阀值，对流量型攻击、连接型攻击、漏洞型攻击及其他各种常见的攻击行为均可有效识别和防护，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

完善设备运维安全保障

- 支持 WEB、SSH2、Console 三种设备管理方式
- 支持 web 页面手动方式软件升级

简洁丰富的 WEB 管理

- 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
- 能够针对攻击进行实时监测，对攻击的历史日志进行方便的查询和统计分析

便捷的抓包取证功能

- 支持自动抓包功能，当受到攻击时，自动抓被攻击主机的报攻击文，便于网络管理人员监控、取证
- 支持指定目标/源 IP 地址、MAC 地址等，用于手动分析攻击类型

高可靠性

- 支持双机热备功能，支持 Active/Passive 工作模式
- 支持集群功能，支持 Active/Active 工作模式，最大可支持 32 台设备集群

产品规格

项目	SecPath AFC2020	SecPath AFC2040	SecPath AFC2100/AFC2100-D	SecPath AFC2200	NSQM1AFCCTI0
接口	1 个配置口（Console） 4 个千兆以太电口 4 个千兆光口	1 个配置口（Console） 2 个千兆以太电口（管理口） 4 个以太网电口 8 个千兆光口	1 个配置口（Console） 2 个千兆以太电口（管理口） 4 个千兆以太光电复用口 2 个万兆光口	\	2 个配置口（Console） 2 个千兆以太电口 4 个万兆光口
外形尺寸（W ×H ×D）	440mm×88mm×500mm（2U 盒式）			490mm×135mm ×435mm（3U 机框式）	

环境温度	工作：0～45℃ 非工作：-40～70℃
环境湿度	工作：10～95%，无冷凝 非工作：5～95%，无冷凝

属性	说明	
攻击防护能力	1.支持对欺骗与非欺骗的 TCP (SYN, SYN-ACK, ACK, FIN, fragments) 、UDP (random port floods, fragments)、ICMP (unreachable, echo, fragments)、(M)Stream Flood 及混合类型攻击的防护。	
	SYN 攻击防御	对欺骗与非欺骗等不同类型的 SYN Flood 攻击支持算法调整功能，在监测到缺省算法无效或者不佳时，可通过人工灵活调整算法；串联模式至少 3 种防护机制，旁路模式至少 5 种，支持真实源探测防护机制；
	UDP 攻击防御	对欺骗与非欺骗等不同类型的 UDP Flood 攻击支持组合防御，在监测到缺省算法无效或不佳时，可通过人工灵活调整防御模式；需具备“业务代理”、“数据包生命周期验证”、“数据包频率限制”、“协议关联验证”、“限时转发”等防御算法，支持真实源探测防护机制；
	ICMP 攻击防御	对非欺骗类型的 ICMP Flood 攻击具备“限时转发”防御算法。
	2.支持链接类型攻击组合防御，在监测到缺省算法无效或不佳时，可通过人工灵活调整防御模式，需包含 Global（客户源）-To-IP（防护主机）模式、IP（客户源）-To-IP（防护主机）模式、IP-To-Port（防护主机）模式和 IP（防护主机）-To-Global（客户源）模式等链接控制功能。	
	3.支持链接类型攻击组合防御，在监测到缺省算法无效或不佳时，可通过人工灵活调整防御模式，需包含“空连接释放”、“连接主动和被动断开次数限制”、“延时提交验证”和“端口关联验证”等防御功能。	
	4.支持链接类型攻击组合防御，在监测到缺省算法无效或不佳时，人员可提取数据包中内容字符，对客户源进行访问频率和并发数量限制，并且能够自动加入动态黑名单。	
	5.提供数据包访问控制功能，能够基于“数据内容长度”、“数据内容字符”、“客户源 IP”、“防护主机 IP”、“协议类型”、“客户源端口”、“防护主机端口”、“TCP Flags”和“TCP Windows size”等条件组合使用，并且能够输出匹配日志和自动加入动态黑名单。	
	6.提供 IP 黑、白名单功能。	
	7.提供网络中未知主机发现功能，能够基于 IP 地址和 MAC 地址对未知主机进行流量限制。	
	8.支持针对 FTP、POP3、SMTP、SSH、HTTP、SSL/TLS 协议类型进行防御，能够根据协议特征自定义防御类型。	
	9.设备具备针对 HTTP 业务提供专用的防护手段，支持文本文件、动态站点等不同级别防御设置，攻击程度较深时可进行手工验证。	
	10.设备具备针对 UDP53、TCP53 及 DNS 提供专用的 DNS Query Flood 防护手段。	
	11.提供流量过滤功能，可根据报文长度、源目 IP、协议、源目端口号、标志位、窗口大小和数据内容等主键对流量进行控制。	
	12.支持对网络中未知的主机，根据 IP、MAC 进行输入和输出流量控制。	
	13.具备对网络中数据包字符相同的流量值限制功能。	
	14.攻击结束后具备攻击事件历史记录，记录需包含攻击源地址、目的地址、目的端口、开始时间、结束时间、持续时间、攻击类型、最大流量和报文档案等信息。	
	15.具备动态黑名单历史分析功能，包含屏蔽时间、源地址、目的地址和屏蔽原因等信息。	
	16.具备动态流量牵引功能，可根据流量值、攻击状态自动在其它路由器或交换机上改变流量走向。	
管理功能	1.管理界面要友好、易用性强，应支持本地管理、远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息。	

属性	说明
	2.系统具备统一管理平台，在集群部署时支持对多台设备的集中管理，日志收集，运行状态监控，策略下发。
	3.针对防御主机 IP 能够进行流量排名、链接排名、攻击状态筛选等功能。
	4.能够根据总流量、输入流量、输出流量、攻击频率、总连接、新建连接进行 TOP 100 过滤。
	5.支持手动和自动报文捕捉功能，手工报文捕捉功能可根据协议类型、源 IP 地址、目的 IP 地址、MAC 地址、采样比等条件进行自定义报文捕捉，捕捉报文可以自动上传 TFTP 服务器。
	6.支持攻击时自动邮件告警功能，邮件信息需要包含攻击源地址、目的地址、目的端口、开始时间等信息。
牵引方式	1.支持静态和动态牵引方式，并且支持 BGP、OSPF 路由协议。
	2.支持二层回注、三层回注、GRE 回注、MPLS LSP 回注、MPLS VPN 回注等多种回注方式。

典型组网

串联与旁路引流应用

H3C SecPath AFC2000 异常流量清洗系统，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，如串联部署模式、旁路部署、双机热备部署和集群部署等。

图1-1 串联部署模式

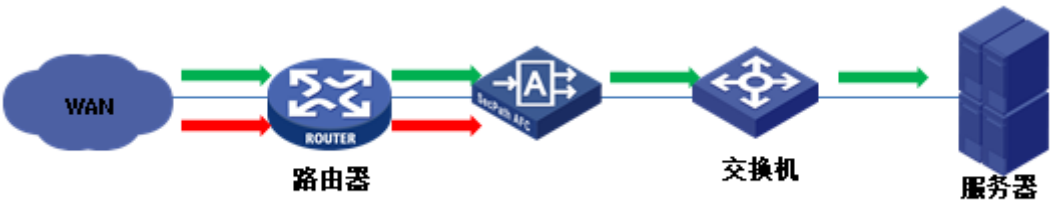


图1-2 旁路模式部署

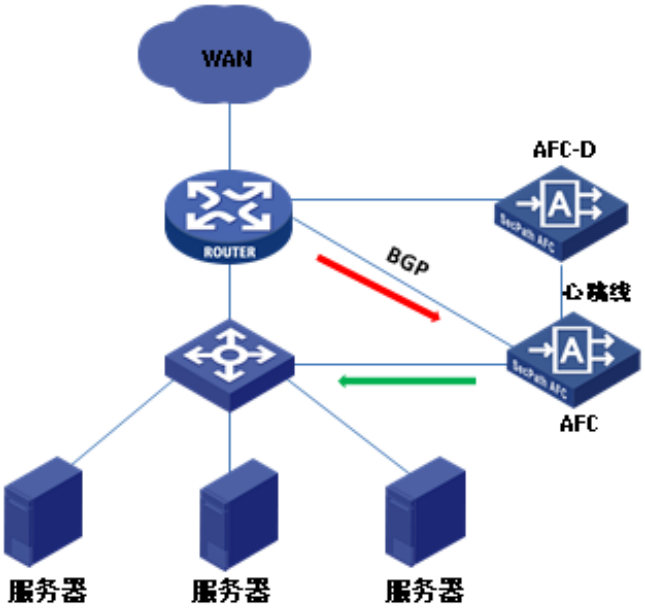
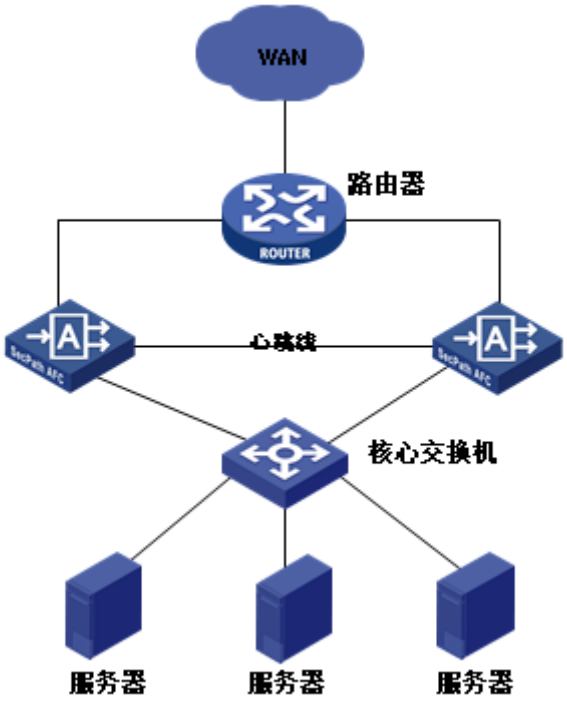


图1-3 双机热备和集群部署



订购信息

H3C SecPath AFC2000 系列产品是 H3C 公司自主开发的异常流量清洗产品，用户可以根据实际需求选购主机和业务板卡。

主机选购

产品	描述	备注
SecPath AFC2020	1 台主机支持 2 组通道	必选
SecPath AFC2040	1 台主机支持 4 组通道	必选
SecPath AFC2100	1 台主机支持 1 组通道	必选
SecPath AFC2100-D	1 台主机支持 1 组通道	必选
SecPath AFC2200	主机箱，3U 机框式	必选，需要配置业务插卡使用，最多可插入两块业务插卡

业务卡选购

模块	描述	备注
NSQM1AFCCTI0	业务卡，支持 2 组业务通道	必选

新华三技术有限公司

北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线
400-810-0504