H3C SecPath AFC2000-G 系列 异常流量清洗与检测产品

产品概述

DH3C SecPath AFC2000 异常流量检测/清洗系统基于 H3C 领先的 ComwareV7 平台，其核心采用自主研发的高效防护算法，主要用于抵抗各类拒绝服务类的网络攻击，针对异常报文攻击、扫描攻击和异常流量攻击等均能够提供有效防护。

H3C SecPath AFC2000-G 系列提供盒式检测系统，盒式清洗系统，和业务处理模块，可针对不同的应用场景，提供不同档位的防护性能。

H3C SecPath AFC2020-D-G 异常流量检测系统为盒式设备，采用了专用的 64 位多核高性能处理器和高速存储器，可以提供高性能的检测能力。

H3C SecPath AFC2000-S-G SecBlade IV 异常流量清洗业务模块和 H3C SecPath AFC2000-G SecBlade IV 异常流量清洗业务模块为可用于分布式主机的业务板，提供上百 G 的异常流量清洗功能。

H3C SecPath AFC2000-G 系列可应用于运营商、IDC 机房，政府、事业单位，大中型企业等，为客户解决拒绝服务类的攻击防护问题，保证安全可靠的网络环境。

H3C SecPath AFC2020-D-G 异常流量检测系统设备外观图

H3C SecPath AFC2120-G 异常流量清洗系统设备外观图

H3C SecPath AFC2000-S-G SecBlade IV 异常流量清洗业务模块外观图

H3C SecPath AFC2000-G SecBlade IV 异常流量清洗业务模块外观图

产品特点

多种攻击防御能力

流量型防御类型

- 支持对 SYN Flood、UDP Flood、ICMP Flood、ACK Flood、DNS Flood、HTTP Flood、SIP Flood 等流量型攻击。
- 支持对 Smurf、Ping of death、Teardrop、IP fragment、Winnuke、Traceroute 等单包攻击。

应用层协议防御

- 支持对 HTTP/HTTPS/DNS/CC 攻击防护。
- 支持自定义协议类型防护特定应用层协议，如对网游、语音、即时通讯相关协议等的防护。
- 支持 HTTP slow header、HTTP slow post、连接数限制等慢速攻击。

防护特性

- 支持针对不同攻击流量启用相应的防护策略，对攻击流量进行相应限制。

- 支持自动识别保护的各个主机及其 IP 地址，并且某台主机受到攻击不会影响其它主机的正常服务。
- 支持根据攻击的流量和连接数阈值来设置自动触发防护选项，并且连接数阈值可根据不同情况灵活控制。
- 支持算法调整功能，即在监测到缺省算法无效或者不佳时，可通过人工调整算法。
- 支持自动和人工添加黑白名单及灵活的规则设置。
- 支持指纹防护，针对数据包头、数据包协议类型及各个字段值、特征自定义频率限制和连接限制功能。
- 支持与 IP 信誉库联动。

域名审计功能

- 支持每域名限速/指定域名限速。
- 支持域名白黑名单功能。
- 分级防护，支持一级与二级域名分开防护，例如：可设置一级域名为放行，二级域名为屏蔽。

牵引回注功能

牵引方式

- 支持静态和动态牵引方式，支持 OSPF 协议、BGP 协议、IS-IS 协议。
- 支持二层回注、策略路由回注、GRE 回注、MPLS LSP 回注、MPLS VPN 回注等多种方式。

丰富的报表

- 提供丰富的报表，主要包括基于攻击事件的报表、基于类型的分析报表等。
- 支持报表以多种格式输出。

完善设备运维安全保障

设备管理

- 支持与管理中心联动。

系统运维

- 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 地址等多种抓包参数，用于手动分析攻击类型。

高可靠性

- 支持电信级业务高可靠性。
- 支持故障隔离：软件模块化技术使软件的各个部分做到故障隔离。H3C Comware 的模块化设计，保证一个进程的异常不会影响其他进程以及内核的正常运行。软件的故障也可以通过自行恢复，不影响硬件的运行。
- 支持进程级 GR：通过完善的进程级 GR 技术，保证异常进程可恢复，并且不影响系统业务。

特性参数

系统配置表

H3C SecPath AFC2020-D-G 异常流量检测系统

项目	描述
名称	H3C SecPath AFC2020-D-G 异常流量检测系统设备系统配置
接口	1个配置口(Console) 2个外置USB host接口 16个千兆以太电口 8个千兆以太光口 2个万兆以太光口
扩展槽	2个，可选PFC接口卡/4端口SFP+接口模块/4端口SFP接口模块
电源	2个电源插槽，支持交流/直流电源模块，不同类型电源不支持混插
外型尺寸（W ×H ×D）	440mm × 44.2mm × 435mm
环境温度	工作：0～45℃(不带硬盘) 非工作：-40～70℃
环境湿度	工作：5%~95%,无冷凝(不带硬盘) 非工作：5%～95%,无冷凝(不带硬盘)

H3C SecPath AFC2120-G 异常流量清洗系统

项目	描述
名称	H3C SecPath AFC2120-G 异常流量清洗系统设备系统配置
接口	1个配置口(Console) 2个外置USB host接口
扩展槽	8个 slot1-3可选2端口QSFP+接口模块/8端口SFP+接口模块/4端口千兆以太网光接口(SFP,LC)+4端口万兆以太网光接口模块(SFP+,LC) slot4-8可选PFC接口模块/8端口GE接口模块/8端口SFP接口模块
电源	2个电源插槽，支持交流/直流电源模块，不同类型电源不支持混插
外型尺寸（W ×H ×D）	440mm × 88.1mm × 660mm
环境温度	工作：0～45℃(不带硬盘) 非工作：-40～70℃
环境湿度	工作：5%~95%,无冷凝(不带硬盘) 非工作：5%～95%,无冷凝(不带硬盘）

AFC2000 SecBlade

项目	描述	
	AFC2000-S-G SecBlade IV	AFC2000-G SecBlade IV
接口	1个配置口(Console) 1个管理网口	1个配置口(Console) 1个管理网口
外形尺寸(W ×H ×D)	399.2mm × 40.1mm × 354.8 mm	399.2mm × 40.1mm × 376.8 mm
环境温度	工作：0～40℃ 非工作：-40～70℃	
环境湿度	工作：5～95%，无冷凝 非工作：5～95%，无冷凝	

接口属性表

设备配置口属性

属性	描述
接头	RJ-45
接口标准	RS-232
波特率	9600～115200bps 缺省9600bps
支持服务	与字符终端相连 与本地PC的串口相连并在PC上运行终端仿真程序 命令行接口
线缆类型	普通异步串行口线缆
传输距离	≤15m

千兆以太网电口属性

属性	描述
接口标准	1000BASE-T
连接器	RJ45
速率	10/100/1000Mbps
工作方式	电口特性：支持10/100/1000M模式、支持MDI/MDIX功能

千兆以太网光口属性

属性	描述
接口标准	1000BASE-X
连接器	LC

速率	1000Mbps
工作方式	光口特性：只支持1000-SX/LX模式，出标准的SFP接口

万兆以太网光口属性

属性	描述
接口标准	10GBASE-R
连接器	LC
速率	10000Mbps
工作方式	出标准的SFP+接口

40GE 以太网光口属性

属性	描述
接口标准	40GBASE-R4
连接器	LC/MPO
速率	40000Mbps
工作方式	出标准的QSFP+接口

功能特性列表

属性	说明	
攻击防护能力	支持网络层防护 支持应用层防护	
	扫描攻击	IP sweep Port scan Distributed port scan
	单包攻击	IP Fragment、IP impossible、Teardrop、Tiny fragment、IP option abnormal、Smurf、Traceroute、Ping of death、Large ICMP、Large ICMPv6、TCP invalid flags、TCP null flag、TCP all flags、TCP SYN-FIN、TCP FIN only flag、TCP Land、Winnuke、UDP bomb、UDP snork、UDP fraggle 等。
	泛洪攻击	SYN flood、ACK flood、SYN-ACK flood、FIN flood、RST flood、UDP flood、ICMP flood、ICMPv6 flood、DNS flood、DNS reply flood、HTTP Flood 、SIP flood 等
	客户端验证	TCP 客户端验证 • Safe Reset • SYN Cookie DNS 客户端验证 DNS reply 验证 HTTP 客户端验证 SIP 客户端验证
	支持防护策略、防护对象管理、防护数据上报	

属性	说明
	支持黑、白名单功能
	支持流量阈值自学习
	支持例外规则
	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
	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对流量进行控制
	支持自定义单包攻击防范策略，可配置IP选项、IPv6扩展头类型等流量特征
	支持多种日志报表
	全面支持IPv6
管理功能	支持通过管理中心进行管理
	针对防御主机IP能够进行流量排名、攻击状态筛选等功能
	能实时显示攻击事件、流量、系统运行状况等信息
	支持手动和自动抓包。
	支持收到攻击时告警
部署方式	串接部署 旁路部署
流量牵引	静态牵引 自动牵引 交互式牵引（BGP、策略路由）
流量回注	二层回注（VLAN） 三层回注（PBR/MPLS隧道/GRE隧道）

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