H3C SecPath AVG2000 防病毒网关

产品概述

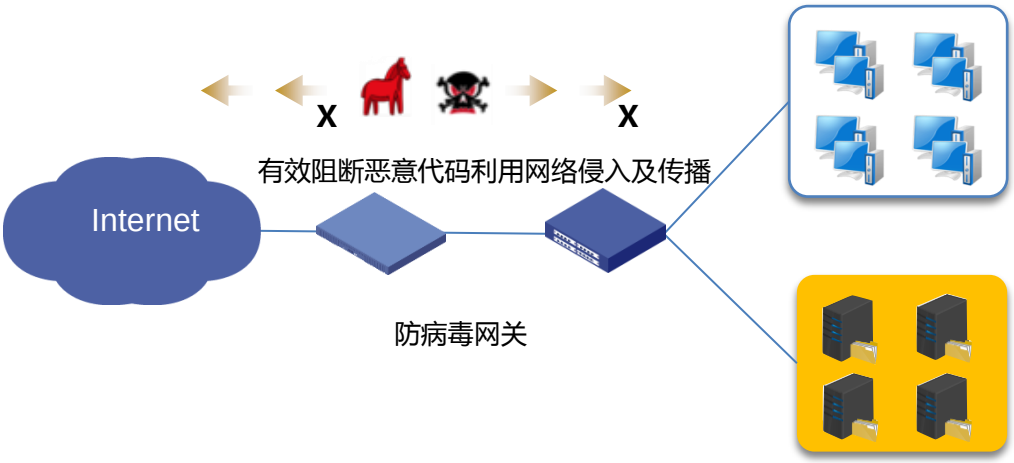
近年来，计算机病毒事件频繁发生，以勒索病毒、挖矿病毒、新型木马、僵尸网络等威胁较为突出，不仅影响到互联网安全，而且也渗透到行业专网致使全网泛滥，造成不可估计的损失与影响。当前新形势下的恶意代码技术不断演变，威胁种类及方式更加多样及流程化，利用网络进行的扩散与攻击则成为病毒蔓延的首要途径，一旦网络遭到突破，内部资产与业务将面临着被恶意加密、丢失、损坏、外泄等危害。

为了实现病毒威胁的全面控制，一个更为有效的控制手段是从网络边界入手，切断传播途径，进行网关级的过滤控制，这样可将被动防御变为积极主动防御，将混合型威胁、阻止在受保护网络之外，为了弥补传统控制方式的不足，新华三技术有限公司自主研发 H3C SecPath AVG2000 系列防病毒网关产品，此产品是针对近年来恶意代码威胁快速演变而设计的一款革新的网关级过滤设备，可全面高效防范恶意代码威胁的传播、动态式攻击、异常通讯，可全面的、综合的覆盖恶意代码威胁的各个阶段，使其无处循形，适用于等级保护、企业内控等信息安全规范，全面保障数据库的完整性、保密性和可用性

H3C SecPath AVG2000 系列防病毒网关产品包括 AVG2000-B、AVG2000-S、AVG2000-A 三个型号，广泛适用于“政府、公安、财政、教育、能源、工商、社保、医疗、国土、金融、运营商、企业”等行业专网或互联网环境。

H3C SecPath AVG2000 系列防病毒网关产品

产品特点



H3C SecPath AVG2000 的部署应用，可将病毒威胁有效拦截在网络边界，提升内网安全，减轻内网安全防护压力。

- 灵活接入，即插即用

H3C SecPath AVG2000 系列防病毒网关产品支持串行、并行、串并混合三种接入模式，即插即用，适应各种复杂的网络环境，支持 VLAN、HA、单臂路由、非对称路由等网络环境。支持无 IP 接入，产品本身不需要设置任何地址即可进行过滤监控。

- IPV4/IPV6 双栈支持

H3C SecPath AVG2000 系列防病毒网关产品全面支持 IPv4 和 IPv6 网络环境。

- 性能优秀，多路监控

H3C SecPath AVG2000 系列防病毒网关产品采用多核并行处理、重构网卡驱动、TCP/IP 协议栈等技术，确保系统的高效过滤性能；支持多路监控，并且可同时支持防御/监测模式的应用。

- 动态识别应用协议

H3C SecPath AVG2000 系列防病毒网关产品支持协议非标准端口的病毒过滤，通讯服务端无论采用什么端口或协议模式，都能正确识别，用户无需手动设定，均可自动化模式匹配。

- 精确的病毒过滤能力

H3C SecPath AVG2000 系列防病毒网关产品针对网络传播病毒进行全面高效的专项过滤，精确识别邮件病毒、文件传输病毒、网页病毒、勒索病毒、手机病毒等，防止病毒通过最常见的传播途径进入受保护网络。

- 强大的蠕虫过滤能力

H3C SecPath AVG2000 系列防病毒网关产品采用入侵防御技术、IP/端口/数据包封锁技术，优化了蠕虫识别机制，不仅可过滤已知蠕虫，还可以在未知蠕虫爆发时通过其行为、速率进行拦截。

- 强大的木马通讯监控

H3C SecPath AVG2000 系列防病毒网关产品内置数千种木马通讯协议识别特征，可监控多样、多类的木马通讯，并通过识别库的不断更新，及时响应新型木马，包括手机木马。

- 强大的僵尸网络通讯监控

H3C SecPath AVG2000 系列防病毒网关产品可识别多种僵尸网络家族及特征，精确定位内部僵尸主机的外联通讯，防护外部“僵尸牧马人”对内部“僵尸主机”的“唤醒、攻击”等指令。

- 全面的内容过滤

支持针对传输文件类型、文件名称、邮件地址、邮件域、邮件主题、附件类型的自定义阻断防护，可保障用户对内部核心文件及信息的审计与防护要求。

- 防范口令探测能力

H3C SecPath AVG2000 系列防病毒网关产品可对常用的网络服务如：SMTP/POP3/IMAP/FTP/HTTP/SMB 等进行口令探测的活动进行监测，并可触发相应的阻断动作，防止口令探测活动的持续进行。并预留接口进行二次开发，对用户专有的网络服务实现口令探测监控。

- 灵活多样的防护策略

H3C SecPath AVG2000 系列防病毒网关产品针对恶意代码类型及形态，具有多种细颗粒度的防护策略，可满足用户针对不同的业务应用，设定不同的防护目标，实现安全与应用的最佳防护体验。

✦ 保障自身安全工作

H3C SecPath AVG2000 系列防病毒网关产品通过多种措施保障自身安全工作：通过专有安全操作系统避免漏洞攻击；通过自动抑制网络流量，防止 DoS 攻击造成拒绝服务和性能下降；通过加密和认证的安全管理防止管理失控。

主要功能

✦ 蠕虫及勒索病毒过滤

蠕虫可以利用电子邮件、网络共享等方式进行扩散，更主要的特点是利用系统的漏洞发起动态攻击。近几年蠕虫造成的危害越来越大，可以导致系统严重损坏和网络瘫痪。如飞客（Conficker）、Wannacry 勒索者病毒等。

根据蠕虫、勒索病毒的特点，H3C SecPath AVG2000 系列防病毒网关产品从 OSI 的多个层次进行处理。在网络层和传输层过滤蠕虫、勒索病毒利用漏洞的动态攻击，在应用层过滤利用正常协议（SMTP、HTTP、POP3、FTP、IMAP、SMB 等）传输的静态蠕虫代码，可实现对恶意代码威胁的动态防御攻击，能够全方位抵御已知蠕虫病毒的攻击，包括所引发的病毒传播、后门漏洞、系统利用攻击等。

✦ 病毒过滤

这里的病毒过滤是指静态型病毒（例如宏病毒）、邮件病毒（例如求职信、美丽杀手、爱虫、Mydoom）、特洛伊木马、网页恶意代码的过滤等。

对于网页浏览（HTTP 协议）、文件传输（FTP 协议）、邮件传输（SMTP、POP3、IMAP 协议）、网络共享（SMB）等病毒，可基于防病毒引擎进行有效识别，并依据策略进行破坏、阻断、隔离等操作。网关内置启发式扫描及深度脱壳病毒引擎，为避免病毒文件传输时利用逃逸和规避手段，网关可自动识别协议工作模式、端口变化、大文件传输、多层压缩文件，用户均无需手动设定，即可通过自动化深度识别与过滤。

- 木马行为监测

一个完整的木马程序包含控制端和被控端。控制者通过操作被控端窃取大量机密或个人隐私信息。H3C SecPath AVG2000 系列防病毒网关产品采用多重特征匹配、模式匹配和规则算法，对网络数据流实时解析，检测出的木马信息包括主机源 IP 地址、MAC 地址、源端口、目的 IP 地址、目的端口、木马类型等信息，对于可疑的木马主机，还可对其上传、下载等行为进行审计与管控。

- 僵尸网络检测

僵尸网络构成了一个攻击平台，控制者利用这个平台可以发起各种各样的恶意攻击，可以导致整个基础信息网络或者重要应用系统瘫痪，也可以导致大量机密或个人隐私泄漏，还可以用来从事网络欺诈等其他违法犯罪活动。

H3C SecPath AVG2000 系列防病毒网关产品采用特征匹配、模式匹配和规则算法，对网络数据流实时解析，检测出僵尸网络发动拒绝服务攻击、发送大量垃圾邮件、窃取计算机上的有用信息、滥用网络资源等恶意的黑客行为，详细信息包括主机源 IP 地址、MAC 地址、源端口、目的 IP 地址、目的端口、僵尸类型、僵尸服务器域名等信息，通过检测信息可以找出内部网络中被种植了“僵尸程序”的“僵尸计算机”以及僵尸的行为。

- 口令嗅探攻击监测

近几年帐号及口令外泄事件时有发生，越来越多的攻击手段也更加明确恶意攻击者的最终目的是要获得核心系统的最高权限，进而更加的肆意妄为。同时，复合型恶意代码或自动化恶意工具在网内执行后，会产生潜在的探测扫描及口令暴力破解等行为。因此，对于信息系统的账户及口令防护，俨然需要提升到一个新的高度，实现对各项信息系统帐户口令的恶意探测及暴力破解等非法行为的实时阻断与监控。

H3C SecPath AVG2000 系列防病毒网关产品通过对信息系统所依赖的网络服务进行协议识别，并深入分析协议层数据包内帐户信息传输状态，进而做到对帐户及口令的有效防御措施，最终实现对信息系统帐户安全的态势分析与全面掌控。

- 分布式集中管理

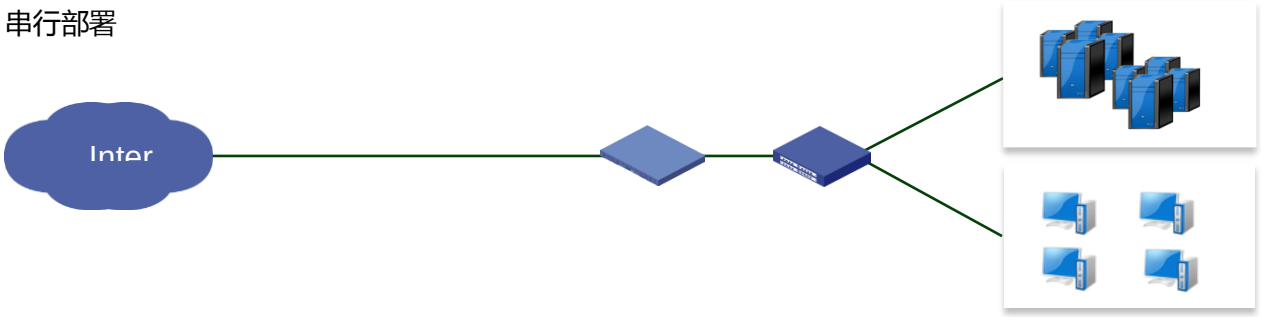
在有多台分布式部署的H3C SecPath AVG2000系列防病毒网关产品场景下，可依据组织架构或节点设定，划分上、下级（或多级）结构，管理员可选任意一台设备作为集控中心，实现对其他设备的集中管控功能，提供特征库的统一升级和策略统一下发，简化日常管理流程，提升日常维护效率。

- 特征库自动升级

H3C SecPath AVG2000系列防病毒网关产品，内置千万级病毒特征库和防御规则库，每日更新2至3次(在线更新)，为用户提供实时的威胁防御能力，及时响应当下最新攻击特征，提供持续有效的、可靠的恶意代码威胁响应及服务。

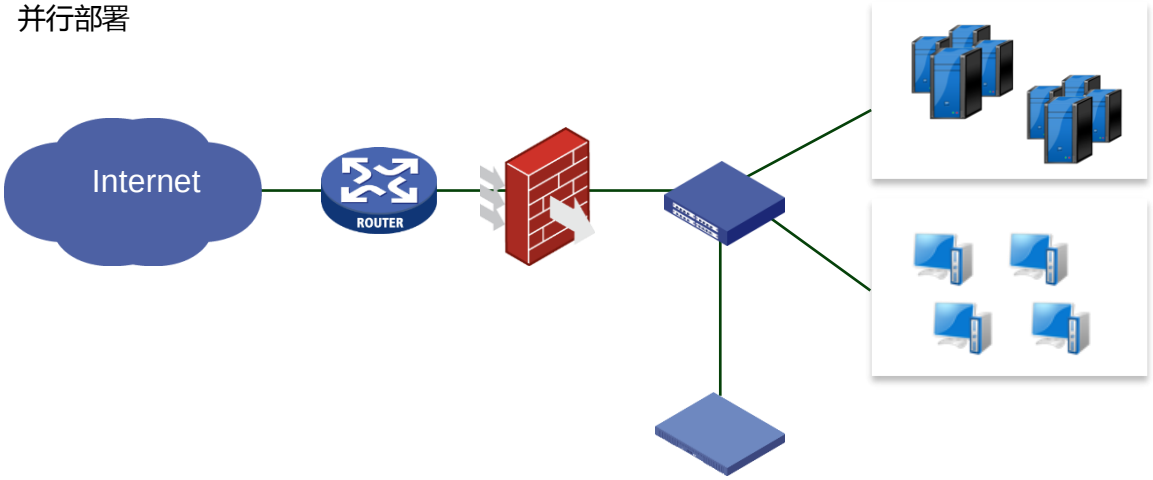
部署方式

- 串行部署



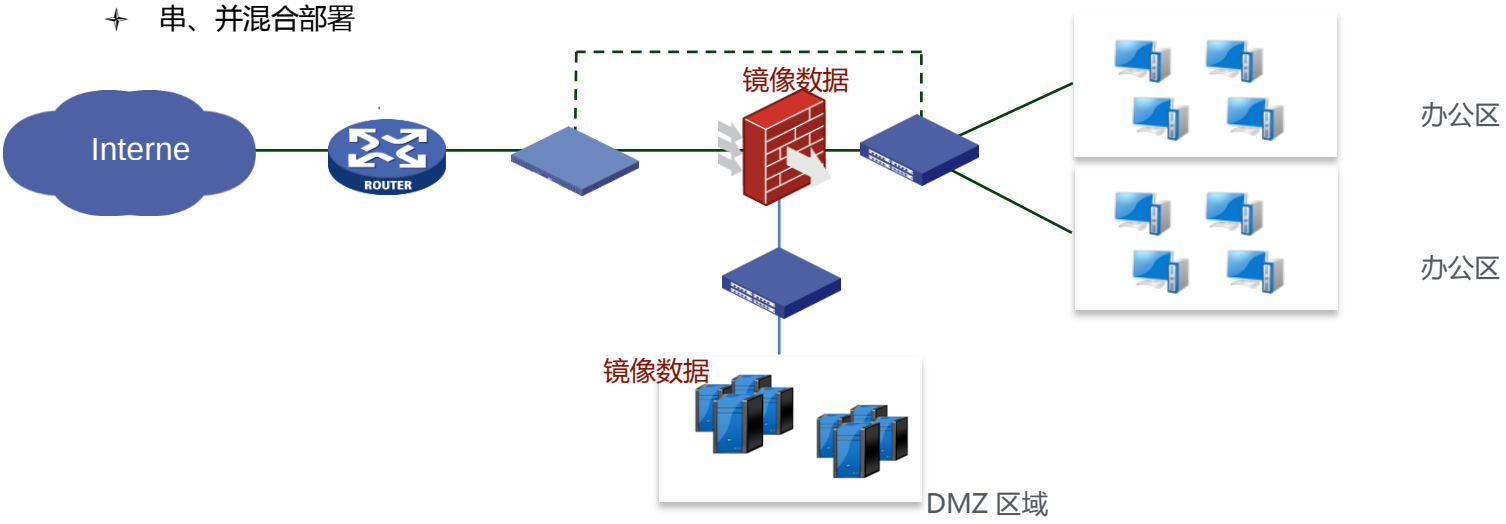
以透明模式串行部署在网络边界处，实现对外部到内部、内部到外部的双向病毒过滤与拦截，保障内网安全。

- 并行部署



通过数据镜像方式，实现对内部威胁的全面监测与精确定位，并行部署对内网威胁纵深监测深度较为全面。

- 串、并混合部署



串并混合部署可满足对安全防御及内网纵深监控的双重要求，实现对恶意代码威胁的多层次覆盖。

产品规格

表1-1 H3C SecPath AVG2000 系列防病毒网关产品规格

属性	AVG2000-B	AVG2000-S	AVG2000-A
规格	2U	2U	2U
扩展槽	2 Slot	4 Slot	8 Slot
部署模式	串行防御、旁路监听、串并混合部署；透明接入、无需变更现有网络结构及配置；支持端口汇聚、VLAN、非对称路由等复杂网络环境。		
链路保障	支持硬件 BYPASS、软件自动 BYPASS、端口连接状态传递。		
协议病毒过滤	支持对 HTTP、FTP、SMTP、IMAP、POP3、SMB 协议双向病毒过滤。		
病毒文件处理	支持对病毒文件的破坏、阻断、隔离、告警、放行操作。		
动态威胁防御	支持蠕虫病毒攻击、勒索病毒攻击、木马通讯、僵尸网络通讯、邮件蠕虫等威胁的综合防御，同时对于上述威胁衍生的次危害如口令探测、暴力破解等		

属性	AVG2000-B	AVG2000-S	AVG2000-A
	行为做到有效抑制和阻断。		
白名单机制	支持病毒名称白名单、五元组白名单、威胁阻断白名单。		
特征库管理	支持在线更新、离线更新、指向更新、定时任务更新等操作。 支持单台设备的特征库分发功能。 特征库更新频率 1-2 次/天，特征库数量达一千万以上。 支持特征库版本回滚功能。		
集中管理	支持单台设备对节点设备的集中管理、分级管理功能。 集中管理功能应具备远程策略下发、配置备份还原、远程 BYPASS 和自动重启、关机等操作。		
设备管理	开放接口	支持 SYSLOG、SNMP、RADIUS、NTP 等协议管理和应用。	
	系统管理	支持Web、CLI方式进行远程配置管理；	
数据分析	风险分析	支持对已有数据的风险分析功能，实现对病毒传播源头、失窃账户信息的呈现。	
	安全报告	支持对威胁事件的安全报告生成、导出，支持doc、pdf、mht格式。	

订购信息

H3C SecPath AVG2000 系列防病毒网关产品是新华三技术有限公司自主开发的产品，用户可以根据实际需求按照型号进行选购。

主机配置

根据产品具体型号选择配置的机箱

表1-2 选购一览表

中文描述	配置选择
H3C SecPath AVG2000-B 防病毒网关设备,含系统软件功能授权函(含一年特征库升级)	必配
H3C SecPath AVG2000-S 防病毒网关设备,含系统软件功能授权函(含一年特征库升级)	必配
H3C SecPath AVG2000-A 防病毒网关设备,含系统软件功能授权函(含一年特征库升级)	必配
H3C SecPath AVG2000-B AVG 特征库升级授权函,1 年	选配
H3C SecPath AVG2000-S AVG 特征库升级授权函,1 年	选配
H3C SecPath AVG2000-A AVG 特征库升级授权函,1 年	选配
H3C SecPath IPC 4 端口千兆以太网光接口模块(SFP,2 Pair Bypass,单模)	选配
H3C SecPath IPC 4 端口千兆以太网光接口模块(SFP,2 Pair Bypass,多模)	选配
H3C SecPath IPC 4 端口千兆以太网电接口(RJ45)+4 端口千兆以太网光接口(SFP)模块	选配
H3C SecPath IPC 4 端口千兆以太网电接口(RJ45,2 Pair Bypass)+4 端口千兆以太网光接口(SFP)模块	选配
H3C SecPath IPC 8 端口千兆以太网电接口模块(RJ45)	选配
H3C SecPath IPC 8 端口千兆以太网电接口模块(RJ45,4 Pair Bypass)	选配
H3C SecPath IPC 8 端口千兆以太网光接口模块(SFP)	选配
H3C SecPath IPC 4 端口万兆以太网光接口模块(SFP+)	选配
H3C SecPath IPC 4 端口万兆以太网光接口模块(SFP+,2 Pair Bypass,多模)	选配
H3C SecPath IPC 2 端口 40G 以太网光接口模块(QSFP+)	选配
H3C 350W 交流电源模块	选配
H3C 550W 交流电源模块	选配

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