华为FireHunter6000沙箱

近年来，众多跨国公司甚至国家政府机构都饱受黑客的攻击，不仅在经济上遭受巨大损失，甚者还对国家安全构成威胁。而攻击者利用的就是0-Day漏洞、高级逃逸技术等多种技术的组合，它们可以绕过现有的大部分安全设备，躲避多层次的网络防护和过滤，最终达到窃取关键信息资产、破坏企业IT基础设施等目的。这种利用先进的攻击手段对特定目标进行长期持续性网络攻击的形式称为APT（Advanced Persistent Threat，高级持续性威胁）攻击。APT攻击通常是定向型攻击，主要攻击涉及国计民生的基础设施，例如能源、金融、交通等。

华为FireHunter6000系列沙箱产品是华为公司推出的新一代高性能APT威胁检测系统，可以精确识别未知恶意文件渗透和C&C（命令与控制，Command & Control，简称C&C）恶意外联。通过直接还原网络流量并提取文件或依靠下一代防火墙提取的文件，在虚拟的环境内进行分析，实现对未知恶意文件的检测。华为FireHunter6000系列沙箱产品面对高级恶意软件，通过信誉扫描、实时行为分析等本地和云端技术，分析和收集软件的静态及动态行为，凭借华为独有的ADE高级威胁检测引擎，华为FireHunter6000系列沙箱产品与下一代防火墙配合，对“灰度”流量实时检测、阻断和报告呈现，有效避免未知威胁攻击的迅速扩散和企业核心信息资产损失，特别适用于金融、政府机要部门、能源、高科技等关键用户。

产品图

华为FireHunter6000系列沙箱产品

HUAWEI

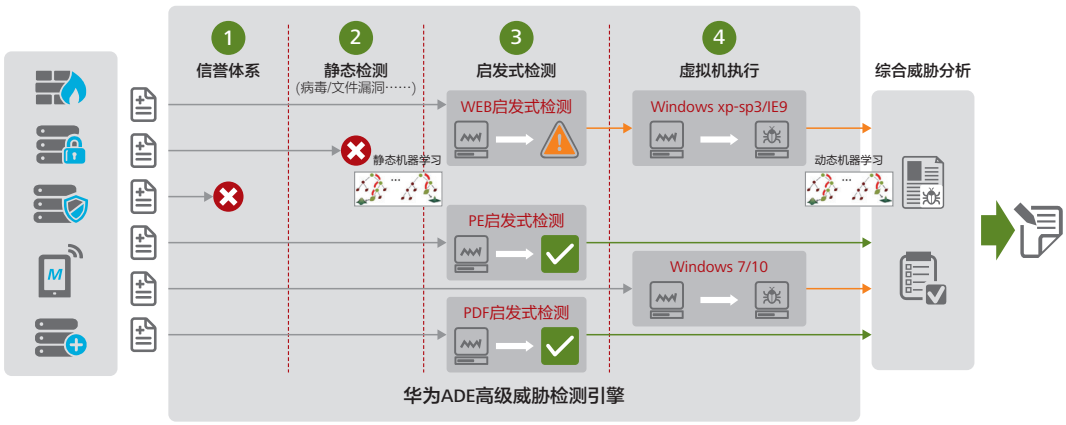
产品特点

50+文件类型检测，全面识别未知恶意软件

- **全面的流量还原检测：**具备业内领先的流量还原能力，可以识别主流的文件传输协议如HTTP、SMTP、POP3、IMAP、FTP、SMB等，从而确保识别通过这些协议传输的恶意文件。
- **支持主流文件类型检测：**支持对主流的应用软件及文档进行恶意代码检测，包括支持PE、PDF、Web、Office、图像、脚本、SWF、COM等50+类型文件的检测。

4重纵深检测，准确性达99.5%以上

- **模拟多种软件运行环境和操作系统：**模拟操作系统和多种软件运行环境：提供PE、PDF、Web启发式沙箱和虚拟执行环境沙箱。虚拟执行环境支持多种Windows操作系统、浏览器及办公软件。
- **动静结合检测：**通过静态分析，包括代码片段分析、文件格式异常、脚本恶意行为分析等，来缩小可疑流量范围；通过指令流监控，识别文件、服务操作，来进行动态分析，最后通过行为关联分析，判断定性。
- **高级抗逃逸：**多种抗逃逸技术，防止恶意软件潜伏、躲避虚拟机检测。



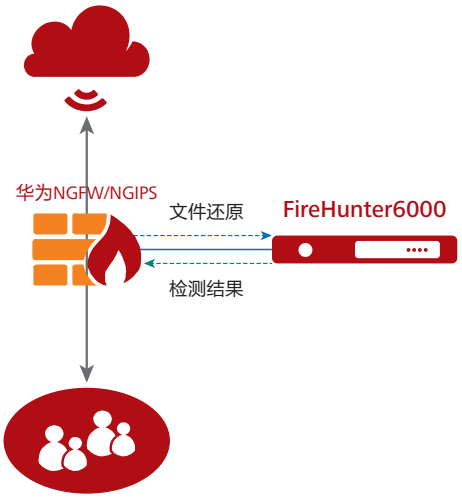
秒级联动响应，快速拦截未知恶意软件

- **业内一流的性能：**提供业内一流的沙箱分析能力，同时支持通过横向扩容方式组成沙箱分析集群。
- **实时的处理能力：**创造性的将对高级威胁的检测和响应时间降到秒级，并通过与下一代防火墙配合实现APT在线防御。
- **提供详细威胁报告，帮助运维、快速决策：**详细展示文件检测结果，包括文件检测结果、文件相关会话信息、文件格式异常、文件行为异常、网络通讯异常、虚拟执行环境信息、网络行为和主机行为等。

产品部署模式

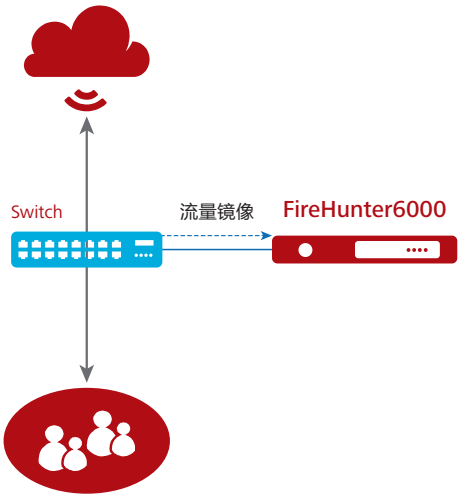
- **与NGFW/NGIPS设备联动部署：**NGFW/NGIPS设备负责还原文件，并将需要检测的文件送到沙箱进行检测。同时NGFW/NGIPS设备还支持SSL流量解密，针对解密后的流量做文件还原，再送沙箱检测。

与防火墙/IPS联动部署



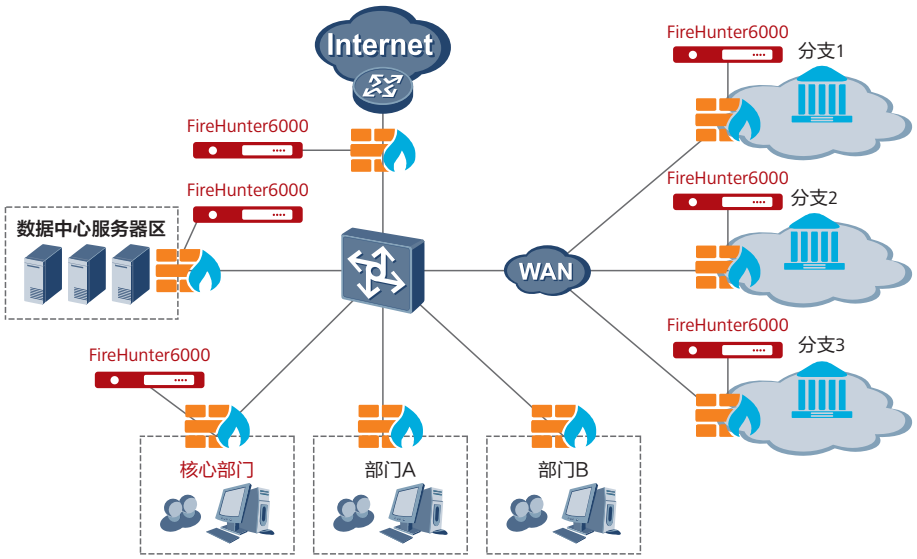
- **单机独立部署：**通过镜像的方式，先将流量镜像到沙箱，沙箱进行流量还原，并对还原出的文件进行检测。

单机独立部署



典型应用

- **互联网边界出口：**重点防范来自互联网的恶意邮件、恶意web流量等。
- **分支接入边界：**避免外联接入区域恶意文件、未知威胁扩散，分支总部之间任意扩散。
- **数据中心边界：**重点保护服务器核心资产，发现内网潜伏的攻击、恶意扫描，渗透等。
- **核心部门边界：**防范内网可疑文件传播，横向感染核心部门。



产品规格

硬件形态		
沙箱型号	FireHunter6000产品系列	
高度	2U	
电源	双冗余电源	
固定接口	8*GE电口（1个千兆管理接口、3个千兆备用接口、4个千兆监听接口），可选2*10GE光口	
主要功能		
类别	**说明**	**详细说明**
支持的操作系统	Windows XP、Win7/10	模拟多种操作系统，虚拟执行环境动态执行检测
支持的流量还原类型	支持多种协议还原	支持HTTP、SMTP、POP3、IMAP、FTP协议的流量还原
支持检测的文件类型	压缩文件	gz，rar，cab，7zip，tar，bz2，zip
	PE	exe，dll，sys（不支持对32位PE格式文件的检测）
	Office97-2003	doc，xls，ppt
	Office 2007及以后	docm，dotx，dotm xmsm，xmtx，xltm，xlam pptm，potx，potm，ppsx，ppsm，ppam
	RTF	rtf
	图片	jpg，jpeg，png，tif，gif，bmp
	WPS	wps，dt，dps
	WEB页面	htm，html，js
	Flash	swf

	JAVA	jar，class
	PDF	pdf
	Python	py，pyc，pyo
	可执行脚本	cmd，bat，vbs，vbe，ruby，ps1，py
内置AV检测	沙箱内置AV，除支持上述检测文件类型，还支持检测chm、asp、php、com、elf格式文件	
C&C异常检测	C&C恶意服务器外联检测	基于DGA域名检测算法，检测C&C外联随机恶意域名
报告输出	输出详细恶意文件检测报告，包括文件检测详情、上威胁行为分类、动态行为分析等	
IOC可机读威胁情报	输出丰富机读情报IOC (Indicators of Compromise)，提供南北向接口共享情报	
尺寸、电源、运行环境		
尺寸 (W × D × H)	86.1mm（2U）× 447mm × 748mm	
重量	净重：28kg 包装材料重量：5kg（11.03lb）	
电源AC	双电源，支持1+1冗余备份，可热插拔 电源额定功率（AC）：550W 额定输入电压（AC）：100V ~ 240V	
电源DC (仅用于FireHunter6300)	双电源，支持1+1冗余备份，可热插拔 电源额定功率（DC）：800W 额定输入电压（DC）：-36V ~ -75V	
工作环境温度	工作温度：5°C ~ 45°C（41°F ~ 113°F） 存储温度：-40°C ~ +65°C（-40°F ~ 149°F） 温度变化每小时小于20°C（36°F）	
海拔	≤3000m，高出900m时，海拔每升高300米工作温度降低1°C	
环境湿度	工作湿度：8% RH ~ 90% RH非凝结 存储湿度：5% RH ~ 95% RH非凝结 湿度变化每小时小于20% RH	

订购信息

编码	描述
主机设备	
FireHunter6100-E-AC	FireHunter6100交流典配E（2*550W交流，滑轨）
FireHunter6200-E-AC	FireHunter6200交流典配E（2*550W交流，滑轨）
FireHunter6300-E-AC	FireHunter6300交流典配E（2*550W交流，滑轨）

编码	描述
接口卡	
CN21ITGAA13	以太网卡-10Gb光口（Intel 82599）-双端口-SFP+（不含光模块）-PCIe 2.0 x8
License	
FH6100-LIC-DCL-1Y	FireHunter6100安全沙箱检测能力库升级服务1年License
FH6100-LIC-DCL-3Y	FireHunter6100安全沙箱检测能力库升级服务3年License
FH6200-LIC-DCL-1Y	FireHunter6200安全沙箱检测能力库升级服务1年License
FH6200-LIC-DCL-3Y	FireHunter6200安全沙箱检测能力库升级服务3年License
FH6300-LIC-DCL-1Y	FireHunter6300安全沙箱检测能力库升级服务1年License
FH6300-LIC-DCL-3Y	FireHunter6300安全沙箱检测能力库升级服务3年License

注：订购清单仅供参考，具体产品订购请咨询华为工程师。