Huawei FireHunter6000 series

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Huawei FireHunter6000 series

FireHunter can detect APT (Advanced Persistent Threat) attacks, which altogether exploit multiple techniques (including zero-day vulnerabilities and advanced evasion techniques), protecting the network against attacks and preventing the internal information from being stolen.

In recent years, many multinational companies and government agencies have been under hacker attacks, suffering great financial loss. Worse still, hacker attacks may lead to national secret disclosure, endangering national security. Attackers exploit a number of techniques altogether, including zero-day vulnerabilities and advanced evasion techniques, to bypass the majority of existing security devices and evade multi-layer network protection and filtering, reaching such purposes as key information stolen and enterprise IT infrastructure damage. Most of such threats aim at targets of great economic or political value, and will cause great danger. They are called Advanced Persistent Threat.

APT attacks are usually target-aimed, mainly attacking the national infrastructure, such as the energy, economy, and transportation. Before launching an attack, an attacker collects the IT information about the target through social engineering, and makes a specific attack plan with the collected information. For example, an attacker finds out the known or zero-day vulnerabilities of the target IT system, and exploits such vulnerabilities to penetrate into the enterprise and spreads threats, finally stealing the key information asset or damaging the IT infrastructure.

FireHunter6000 Sandbox is Huawei's new high-performance APT detection system. By restoring the network traffic mirrored by switches or traditional security devices, FireHunter6000 Sandbox inspects files transmitted on the network in virtual environments to detect malicious files. Facing advanced malware, FireHunter6000 Sandbox analyzes and collects the static and dynamic software behaviors through local and cloud techniques, such as reputation scanning, real-time behavior analysis, and big data correlation. With the unique behavior pattern library, FireHunter6000 Sandbox can obtain accurate analysis results, and detect, report, and block "grey" traffic in real time to control the spreading of unknown threats and loss of core information assets of enterprises. FireHunter6000 Sandbox is particularly applicable for major customers like financial institutions, confidential government agencies, energy companies, and high-tech enterprises.

Product Appearances

FireHunter6000 series

Product Overview

FireHunter6000 has multiple built-in sandbox systems, which can run the programs to be analyzed, collect static and dynamic program behaviors, and display the behaviors to users, showing users whether the program is malicious. The unique technology of behavior pattern library is what the FireHunter6000 uses to finish the above process. Through feature analysis of a large quantity of viruses, vulnerabilities, and threats, FireHunter6000 summarizes the malicious behavior pattern and develops a set of judgment rules, each rule defining one or more software behaviors. According to the rules matching software behaviors of the inspected programs, FireHunter6000 will display the corresponding detection results.

Heuristic sandbox types that FireHunter6000 supports:

PE heuristic sandbox: The PE heuristic sandbox is used to inspect Windows executable files. It can build a virtual execution environment by simulating hardware instructions, and run PE files in the virtual environment to collect file behaviors. Compared with the virtual execution environment at the operating system level, the PE heuristic sandbox is a heuristic sandbox at the process level with higher file analysis performance.

PDF sandbox: The PDF sandbox is used to inspect PDF files. By simulating the PDF file reader program, the PDF sandbox can analyze the behaviors of PDF files. Compared with the virtual execution environment at the operating system level, the PDF sandbox is a heuristic sandbox at the process level with higher file analysis performance.

Web sandbox: The web sandbox is used to inspect web page files. By simulating the browser program, the web sandbox can analyze the behaviors of web files. Compared with the virtual execution environment at the operating system level, the web sandbox is a heuristic sandbox at the process level with higher file analysis performance.

Virtual execution environment: Virtual execution environment, compared with heuristic sandboxes, has a relatively lower detection rate while higher detection quality. Heuristic sandboxes can detect malicious files according to their malicious signatures. However, many malicious files can hide their malicious signatures, showing malicious behaviors only when run. To overcome the disadvantage of heuristic sandboxes, FireHunter6000 also provides the virtual execution environmentto detect the above threats. The virtual execution environment is a real operating system based on the virtual machine technology. When running in the virtual execution environment, files to be inspected can use any API interface of the system, just like on the real host. FireHunter6000 will monitor the running process of the files, and detect malicious files according to the behavior signatures. When suffering destructive impact from malicious files, the virtual execution environmentwill automatically restore the virtual environment to initial status, leaving no impact on the inspection performance of FireHunter6000.

Highlights

Multi-System Simulation and Comprehensive Inspection, Preventing Unknown Threats and Malicious Software

Comprehensive traffic inspection: FireHunter6000 Sandbox can restore the traffic and identify such mainstream file transfer protocols as HTTP, SMTP, POP3, IMAP, and FTP, ensuring the detection of malicious files transmitted using these protocols.

Inspection support of mainstream file types: FireHunter6000 Sandbox supports malicious code detection of mainstream application software and files, including Word, Excel, PPT, PDF, HTML, JS, EXE, JPG, GIF, PNG, SWF, and ZIP.

Inspection support of web traffic: Among all the detection systems of the same type in china, FireHunter6000 Sandbox is unique in detecting web-based malicious code and zero-day vulnerabilities of web pages. Even globally, only two companies can provide such inspection, greatly improving the detection

efficiency of unknown threats of FireHunter6000.

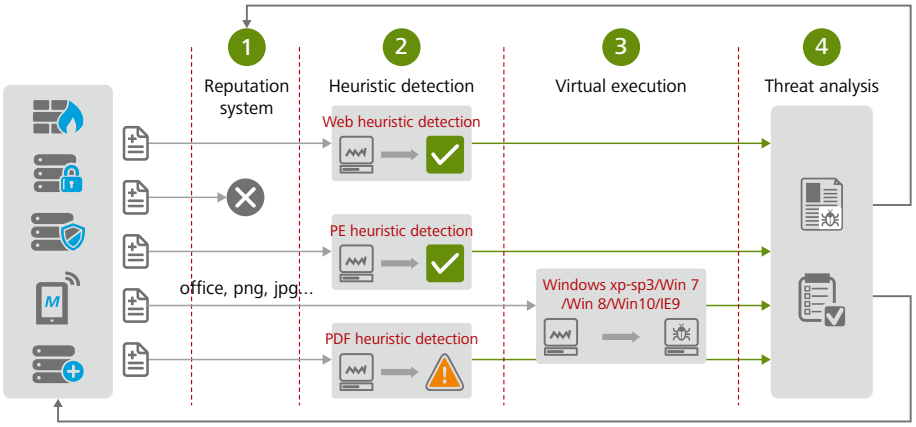
Simulation of mainstream operating systems and application software: FireHunter6000 Sandbox can simulate mainstream operating systems and software, including Windows operating systems, browsers like Internet Explorer, and office software like Microsoft Office and WPS. In addition, FireHunter6000 Sandbox can customize virtual environments based on user requirements.

In-depth Inspection and Second-Level Response, Rapidly Blocking Unknown Threats and Malicious Software

Layered defense system: FireHunter6000 Sandbox supports reputation matching, heuristic detection, and virtual execution, equipped with a quick response to the next-generation threats represented by APT.

Industry-leading performance: FireHunter6000 Sandbox has an industry-leading analysis capability, with 70 thousand samples analyzed per day. Meanwhile, FireHunter6000 Sandbox supports horizontal capacity expansion, which can form analysis clusters to further improve analysis capability.

Quasi real-time processing: FireHunter6000 Sandbox has a quasi real-time processing capability, reducing response time of next-generation threat detection from several weeks to few seconds, and interworking with the NGFW to implement online defense.



Multi-Dimensional Analysis and Less False Positives, Accurately Detecting Unknown Threats and Malicious Software

Multi-dimensional analysis: Huawei FireHunter performs static analysis of code snippets, file format anomalies, and malicious script behavior to pin down suspicious traffic; performs dynamic analysis through instruction stream monitoring to identify malicious files and operations; performs correlated behavior analysis to determine whether traffic is legitimate.

Deployment Mode

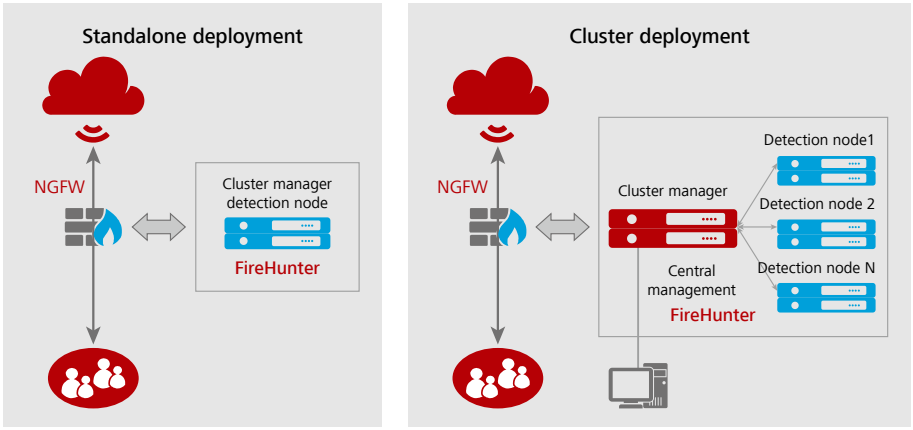
FireHunter6000 Sandbox supports multiple deployment modes.

Interworking with the NGFW, standalone deployment: The NGFW restores files and sends files to be detected to the sandbox.

Interworking with the NGFW, cluster deployment: The NGFW restores files and sends files to be detected to the sandbox cluster. Four FireHunter V100R001C20s or FireHunter V100R001C30s can be deployed in a

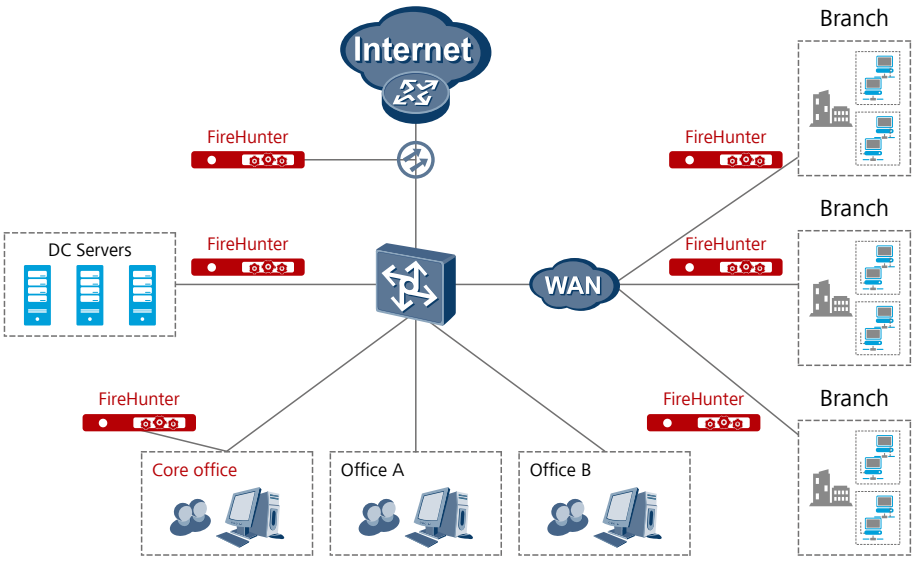
cluste. In a cluster, a device serves as the management center, and other devices the detection nodes. The management center distributes files to detection nodes for load balancing and provides a unified detection result query interface.

Standalone deployment: Traffic is mirrored to the sandbox, which restores the traffic to files and detects them. Traffic can be mirrored using the mirroring port or optical splitter. In this scenario, the sandbox only detects files, and other security devices block files.



Typical Deployment

1. **Internet egress:** To mainly defense malicious mails and web traffic from the Internet.
2. **Branch access border:** To prevent malicious files and unknown threats in external access zones from spreading between branches and HQ.
3. **Data center border:** To mainly protect core assets of servers and discover attacks hiding on the internal network, malicious scanning, and penetration.
4. **Core department border:** To prevent suspicious files from spreading on the internal network and horizontally infecting core departments.



Specifications

Hardware configuration		
Model	FireHunter6000	
Hardware configuration	• x86 server in a 2-U rack • Memory of no less than 128 GB • Two power modules for redundancy • Hard drive with a capacity of no less than 2 TB • SSD drive with a capacity of no less than 128 GB • 8 x GE electrical ports • 2 x 10GE optical ports	
Main Functions		
PE file inspection		
	32-bit PE file inspection	Yes
	Compressed PE file inspection	Yes
PDF file inspection		
	PDF file inspection	Yes
	Compressed PDF file inspection	Yes
Web file inspection		
	HTML/HTM file inspection	Yes
	JavaScript file (contained in HTML/HTM files) inspection	Yes
	Flash file inspection	Yes
	JavaApplet file inspection	Yes
	Compressed web file inspection	Yes
Office file inspection		
	Word 2003 and Word 2007 inspection	Yes
	Excel 2003 and Excel 2007 inspection	Yes
	PowerPoint 2003 and PowerPoint 2007 inspection	Yes
	RTF file inspection	Yes
	Office file (attached to mails) inspection	Yes
	WPS file inspection	Yes
	Compressed Office file inspection	Yes
Image inspection		
	GIF file inspection	Yes
	JPG file inspection	Yes

Hardware configuration		
	PNG file inspection	Yes
	TIFF file inspection	Yes
	Compressed image inspection	Yes
Traffic restoration		
	http, smtp, pop3, imap, ftp protocol traffic restoration	Yes
Deployment mode		
	Local deployment, interworking with the NGFW	Yes
	Local out-of-path deployment	Yes
	Cluster deployment	Yes

Ordering Information

Host	02311GVW	Function Module, FireHunter6000, FireHunter6300-AC, FireHunter6300 AC Typical Configuration(2*750 AC PSU, Static Rail Kit)
License	88033DNR	Software Charge, FireHunter6000, FH6000-LIC-1AV-1Y, One-year single-engine antivirus library update license of FireHunter, Multiple Model
License	88033DNT	Software Charge, FireHunter6000, FH6000-LIC-1AV-3Y, Three-year single-engine antivirus library update license of FireHunter, Multiple Model
License	88033DNX	Software Charge, FireHunter6000, FH6000-LIC-TML-1Y, One-year threat model library update license of FireHunter, Multiple Model
License	88033DPA	Software Charge, FireHunter6000, FH6000-LIC-TML-3Y, Three-year threat model library update license of FireHunter, Multiple Model

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P.R. China
Tel: +86-755-28780808

Version No.: M3-032102-20161220-C-1.0

www.huawei.com