# HUAWEI FireHunter V100R001 Product Description

Issue 01
Date 2017-03-24

# • Product Values •

## Product Positioning

Huawei FireHunter sandbox is a high-performance APT detection system that combines the multi-engine-based virtual detection technology with the traditional security detection technology to identify malicious files and C&C attacks spreading across the network. It effectively makes up for the deficiency of traditional signature-based detection methods, preventing unknown threats from spreading and protecting core information assets for enterprises. It applies especially to key users from finance, government, energy, and high-tech sectors.


## Product Features

### Reduce security risks

- Comprehensive traffic detection
- Independent traffic restoration
- Near real-time processing

Quick response

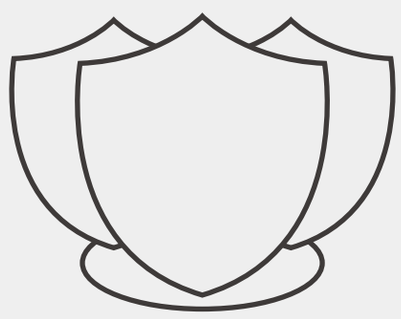
### Improve detection capability

- Layered detection system
- Static code analysis
- Dynamic virtual execution

Static and dynamic combined

### Eliminate potential threats

- APT attack path display
- Interworking with conventional security devices
- Full-fledged protection system



Collaborative defense

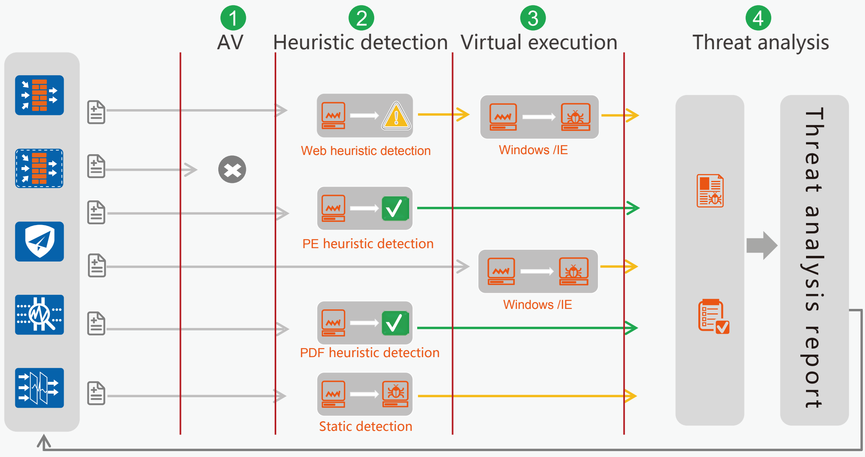
## Comprehensive traffic detection

Simulate mainstream operating systems and application software for the detection of mainstream files.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Identified protocols | HTTP | SMTP | POP3 | IMAP | FTP | NFS | SMB |
| Identified files | Web | Flash | PDF | CHM | WPS | MS Office | |
| | PE | ELF | Script | URL | Image | Compress | |
| Simulated operating system | WinXP | Win7 | Win10 | | | | |
| Simulated browser | IE | Chrome | | | | | |
| Simulated Office software | Microsoft Office | WPS Office | | | | | |
| Simulated Adobe Reader | 8 | 9 | X | XI | | | |

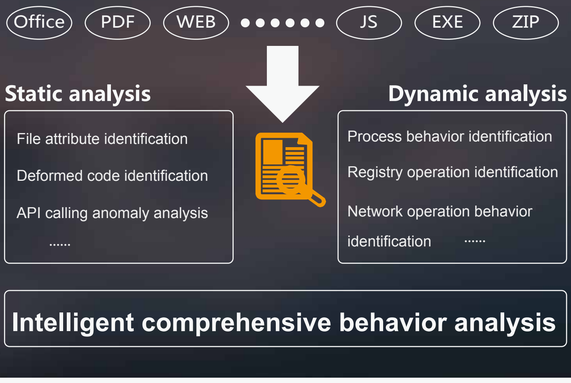
## Layered detection system

The FireHunter sandbox system employs a multi-layer malicious file behavior detection mechanism that uses the signature database, heuristic detection engine, and virtual execution environment technology to perform in-depth detection on unknown files and discover potential attacks in a timely manner.



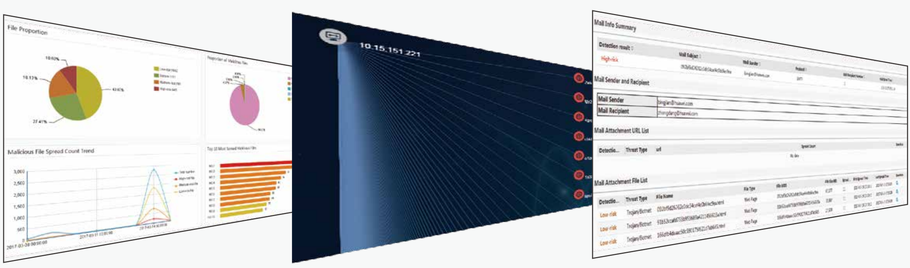

## Multi-dimensional threat analysis

Huawei FireHunter sandbox performs static analysis to pin down suspicious files, employs dynamic analysis to identify files and operations, and determines whether the files are illegitimate ones through intelligent behavior analysis.

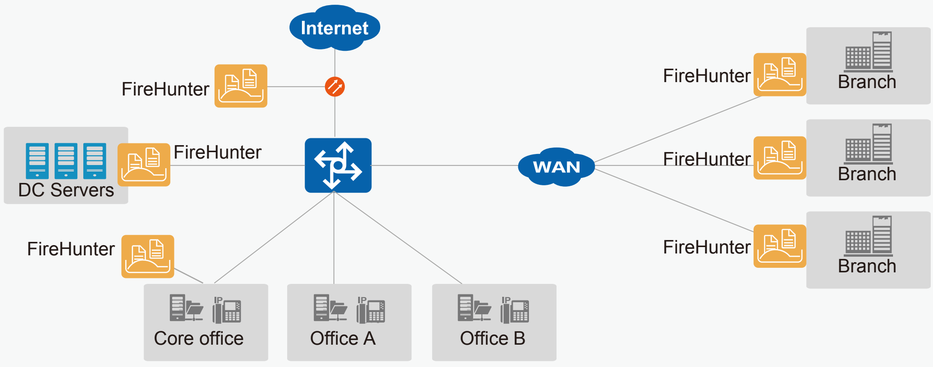



## Displays of diversified threat scenarios

The FireHunter supports the display of threat spread paths and behaviors in mail, web, and C&C scenarios.

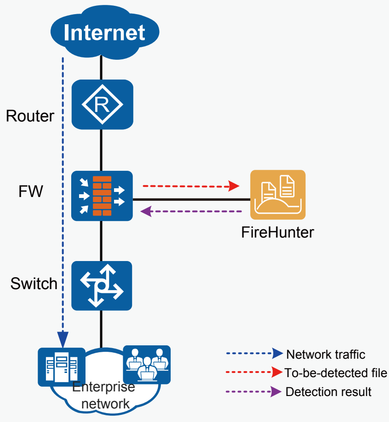


# Deployment location



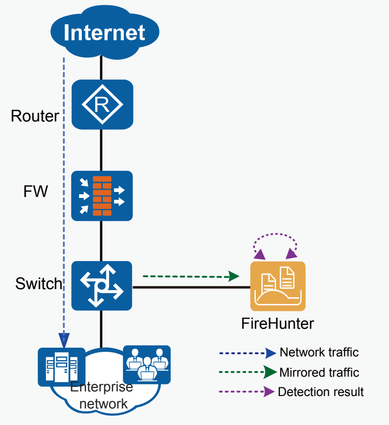

- **At the Internet egress**: defend against attacks from the Internet, such as malicious emails and web traffic attacks.
- **Between branches**: prevent the spread of malicious files from external networks and avoid the spread to other branches or even headquarters.
- **At the boundaries of core departments**: prevent the spread and share of suspected files in the intranet to protect core departments.
- **At the boundary of the data center**: protect core assets on servers by preventing attacks, malicious scan, penetration, and other threats in the intranet.

# Deployment scenario



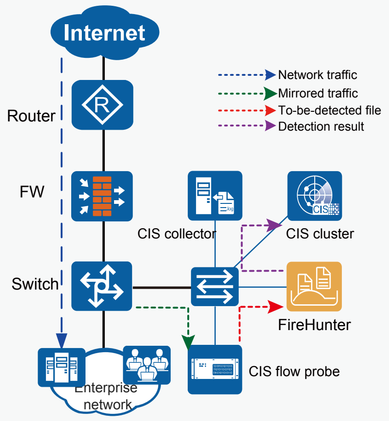

## Interworking with the firewall

- The firewall is deployed at the network egress, and extracts files from the network traffic and sends the files to the FireHunter for threat detection. After the detection completes, the firewall queries the detection result from the FireHunter and determines security policies accordingly. The administrator can view the detection result on the FireHunter web UI.
- By interworking with the firewall, the FireHunter enables the enterprise network to defend against both known and unknown security threats, including malicious files and websites, enhancing the security of the entire network.




## Off-line deployment for traffic restoration

- The FireHunter is attached in off-line mode to a switch. The switch mirrors network traffic to the FireHunter. Then the FireHunter restores the network traffic into files for threat detection. Meanwhile, the FireHunter also performs C&C threat detection on the mirrored traffic. The administrator can view the detection result on the FireHunter web UI.
- In this deployment, the FireHunter only detects threats in the traffic, and other security devices block the threat traffic.

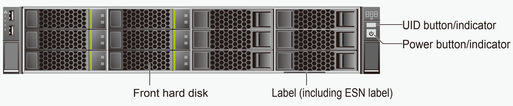



## Interworking with the CIS

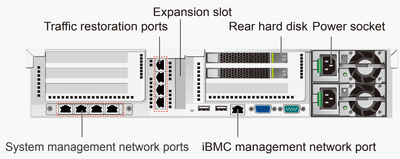
- The FireHunter is deployed together with the cybersecurity intelligence system (CIS). The CIS flow probe receives and restores network traffic mirrored by the switch, extracts restored files, and sends them to the FireHunter for threat detection. After the detection completes, the FireHunter sends the detection result to the CIS cluster through the CIS collector. The CIS cluster summarizes and analyzes threat logs and anomaly events reported by the FireHunter and other network devices and displays the entire APT attack process and network-wide security posture on the web UI.
- The FireHunter is deployed together with the CIS to improve the user network's capability of defending against various APT attacks.

# Appearance

Front panel




Rear panel




| Name | Description |
|---|---|
| Power button /indicator | • Off: The server is not powered on.<br>• Blinking yellow: The iBMC is being started.<br>• Steady yellow: The system is in the standby state.<br>• Steady green: The system is properly powered on. |
| UID button/indicator | The UID button/indicator helps identify and locate a server in a rack. You can turn on or off the UID indicator by manually pressing the UID button or remotely running a command on the iBMC CLI. |
| Front hard disks | 6 x 2TB SATA, numbered 0 to 5 from top to bottom and from left to right.<br>• System hard disk: Slot 0 to 1 (RAID1)<br>• Data hard disk: Slot 2 to 5 (RAID10) |
| System management network ports | The ports are numbered ETH0 to ETH3 from left to right and apply to the interworking scenario. |
| Traffic restoration ports | The traffic restoration ports only apply to the traffic restoration scenario and are numbered ETH4 to ETH7 from top to bottom. |
| Expansion slot | Expansion slot is reserved for expansion cards to provide more 10GE ports or functions. The ports only apply to the traffic restoration scenario. |
| iBMC management network port | The port is used to login the iBMC. |
| Rear hard | Mirroring hard disk: 2 x 200 GB SSD (RAID1) |
| Power socket | Double hot-swappable DC or AC power modules working in 1+1 backup mode. |

# Physical Specifications

| Item | Specifications |
|---|---|
| **System parameters** | |
| CPU | 2*E5-2620 v3 |
| Memory | 16*16GB |
| Front hard disk | 6 x 2TB SATA |
| Rear hard | 2 x 200 GB SSD |
| Hard disk hot-swap | Supported |
| Hard disk expansion | Not supported |
| **Dimensions and weight** | |
| Dimensions (H x W x D) | 86.1 mm (2 U) x 447 mm x 748 mm (3.39 in. x 17.60 in. x 29.45 in.) |
| Installation space | The server fits into a universal rack complying with the IEC 297 standard.<br>•Rack width: 19 inches<br>•Rack depth: > 1000 mm (39.37 in.)<br>Guide rail installation requirements are as follows:<br>•L-shaped guide rails: apply only to Huawei cabinets.<br>•Adjustable guide rail: The distance between the front rear mounting bars is 543.5 mm to 848.5 mm. |
| Weight | Net weight: 28 kg (61.73 lb)<br>Packing material weight: 5 kg (11.03 lb) |
| **Power supply parameters** | |
| AC power | Double hot-swappable AC power modules working in 1+1 backup mode. |
| PSU power rating (AC) | 750 W |
| Rated input voltage (AC) | 100 V to 240 V AC |
| DC power | Double hot-swappable DC power modules working in 1+1 backup mode. |
| PSU power rating (DC) | 800 W |
| Rated input voltage (DC) | -36V to -75V |
| **Environmental parameters** | |
| Temperature | Operating temperature: 5°C to 45°C (41°F to 113°F)<br>Storage temperature: -40°C to +65°C (-40°F to +149°F)<br>Temperature change rate: < 20°C/h (36°F/h) |
| Altitude | ≤ 3000 m (9842.40 ft). When the altitude is higher than 900 m (2952.72 ft), the operating temperature decreases by 1°C (1.8°F) per 300 m (984.24 ft). |
| Humidity | Operating humidity: 8% RH to 90% RH (non-condensing)<br>Storage humidity: 5% RH to 95% RH (non-condensing)<br>Humidity change rate: < 20% RH/hour |
| Acoustic Noise | The data listed in the following is the declared A-weighted sound power levels (LWAd) and declared average bystander position A-weighted sound pressure levels (LpAm) when the server is operating in a 23°C (73.4°F) ambient environment. Noise emissions are measured in accordance with ISO 7999 (ECMA 74) and declared in accordance with ISO 9296 (ECMA 109).<br>·Idle:<br>−LWAd: 5.1 Bels<br>−LpAm: 35.1 dBA<br>·Operating:<br>−LWAd: 6.1 Bels<br>−LpAm: 45.1 dBA<br>NOTE:<br>The actual sound levels generated during server operating vary depending on the server configuration, load, and ambient temperature. |

# · Product Specification ·

## Product Functions

| Feature | Description |
|---|---|
| Traffic restoration | Supports independent traffic restoration to identify mainstream network protocols, such as HTTP, SMTP, POP3, IMAP, FTP, NFS, and SMB. |
| | Supports C&C threat detection that based on remote control tool features and on DGA domain name access. |
| File detection | Supports the detection of mainstream files, such as Microsoft Office, web, URL, Flash, PDF, CHM, script, executable, image, compressed, and WPS files. |
| | Supports the detection of files from multiple sources, including files that are submitted by the interworking device, restored from mirrored traffic, and manually submitted. |
| Detection mechanism | Supports the antivirus engine and signature database for detection of known viruses on sample files. |
| | Supports the heuristic detection engine capable of heuristic detection on web, PE, and PDF files with a high processing performance. |
| | Supports the static detection engine. |
| | Supports the virtual execution environment that can simulate a real operating system, monitor the behavior of the process corresponding to the to-be-analyzed file, and determine on whether the file is malicious based on its behavior features. |
| | Supports the summarization of the preceding detection results for intelligent and comprehensive analysis, based on which a score and a threat level are given. |
| Threat visualization | Supports the display of web threat scenarios. |
| | Supports the display of mail threat scenarios. |
| | Supports the display of C&C threat detection results. |
| | Supports the display of file detection results and reports. |
| Threat report | Supports the display of statistics on the threat trend, malicious files, malicious domain names, attacked hosts, malicious websites, system status, and file analysis. |
| | Supports the batch export of detection reports, machine-readable IOC intelligence, and detection results. |
| Smart search | Supports the search based on the log event field and keyword. |
| | Supports the search based on multiple combined conditions. |
| | Supports the display of search result details. |
| Visualized management and maintenance | Supports one-click information collection to obtain device status information and save it to the local device. |
| | Supports local and online update of resources, such as the signature database, behavior pattern library, and detection engine. |
| | Supports user management, including user adding, deletion, and modification. |
| | Supports the sending of threat logs and the usage of a log server for log collection and management. |
| | Supports license-based management. |