华为 HiSecEngine IPS6000F 系列

新一代入侵防御系统彩页

1 产品概述

华为 HiSecEngine IPS6000F 系列产品是华为推出的新一代专业入侵防御产品，主要应用于企业、IDC、校园网和运营商等，为客户提供运营安全保障。

HiSecEngine IPS6000F 系列产品在传统 IPS 产品的基础上增加了对被检测内容、深度应用和网络环境的感知能力，以及对未知威胁的防御能力，实现更精准的检测能力，和更优化的管理体验。全方位保障客户应用和业务安全，实现对网络基础设施、服务器、客户端以及网络带宽性能的全面防护。

2 产品外观

图1 华为 HiSecEngine IPS6525F

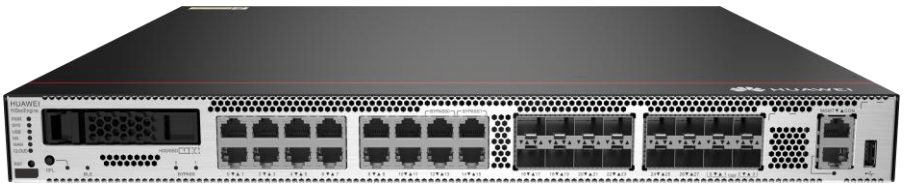


图2 华为 HiSecEngine IPS6585F/IPS6615F

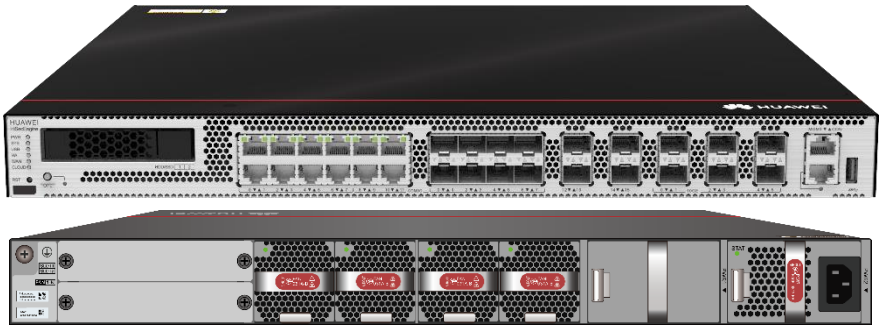


图3 华为 HiSecEngine IPS6625F

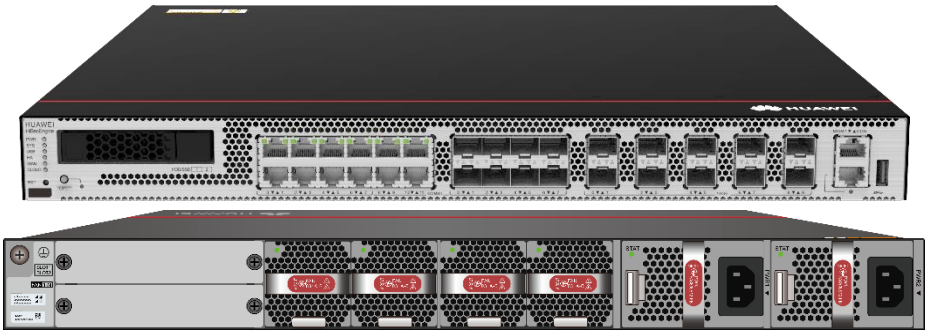
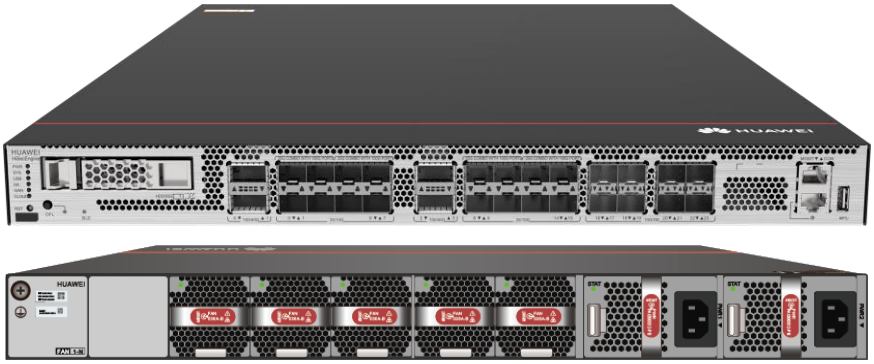


图4 华为 HiSecEngine IPS6655F



3 产品亮点

全新软硬件架构，检测性能进一步提升

- 硬件采用专用多核平台，大大提高产品检测性能
- 软件方面采用全新的 IPS 检测引擎进行威胁检测，多重防护并行处理，极大提升了威胁检测性能

多重检测，全面防护

- 提供对系统、应用、恶意软件以及客户端攻击最精准的保护
- 识别 120+真实文件类型，防扩展名篡改，识别文件中的恶意代码
- 应对面向 HTTP、DNS、SIP 等应用的拒绝服务攻击，提供业界领先的应用层 DDoS 防护功能

签名更新快，漏洞及时防御

- 专业的签名开发团队密切跟踪全球知名安全组织和软件厂商发布的安全公告，并遵从国际权威组织 CVE 的兼容性认证要求，对这些威胁进行分析和验证
- 通过遍布全球的蜜网，实时捕获最新的攻击、蠕虫病毒、木马等，提取威胁的特征，发现威胁的趋势
- 华为能够在最短时间内发布最新的签名，及时升级检测引擎和签名库

4 产品硬件规格

型号	IPS6525F	IPS6585F	IPS6615F	IPS6625F	IPS6655F
固定接口	16*GE(RJ45) + 12*GE(SFP) + 4*10GE(SFP+)	8*GE COMBO + 4*GE(RJ45) + 4*GE(SFP) + 6*10GE(SFP+)		8*GE COMBO + 4*GE(RJ45) + 10*10GE(SFP+)	4*100GE(QSFP28) + 16*25GE(ZSFP+) + 8*10GE(SFP+)
USB 口	1×USB2.0	1×USB3.0			
硬盘	选配，2.5 英寸 SATA 硬盘 240GB/480GB/960GB/1920GB，可热插拔				
Bypass 插卡	支持，2 块电 BYPASS 或光 BYPASS				不支持
机箱高度	1U				
尺寸(W×D×H,单位 mm)	442 x 420 x 43.6				442 x 600 x 43.6
风扇	1+1	3+1			4+1
散热（气流走向）	前面板进，后面板出				
最大功耗	123W	222W		242W	445W
电源输入电压（AC）	100V～240V，AC 50Hz/60Hz				
电源冗余	选配			标配	
重量(空配)	7.2kg	6.3kg		7.3kg	10.6kg
工作环境	温度：0℃～45℃				

	湿度：5%RH～95%RH，无冷凝
存储环境	温度：-40℃～70℃
	湿度：5%RH～95%RH，无冷凝

5 功能特性

功能特性	
安全策略	支持基于 VLAN ID、五元组、安全域、地区、应用和时间段等维度对流量进行管控，并同时进行内容安全的一体化检测。
应用识别与管控	非基于端口，基于签名、关联识别、行为识别等技术进行识别；预置 6000+应用，支持细分应用，例如：区分微信的文字和语音；支持自定义应用；支持 50+的分类和 20+的风险标签，可基于分类及标签进行访问控制；并支持应用识别特征库自动升级。
入侵防御	第一时间获取最新威胁信息，准确检测并防御针对漏洞的攻击；支持万级 CVE 漏洞覆盖；支持漏洞攻击、Web 攻击 (如 SQL 注入、跨站脚本攻击等)、僵尸网络/远控/木马等恶意流量的检测，支持基于用户行为的暴力破解检测；支持自定义签名；预定义签名数最大 2.5 万+，并支持特征库自动更新；支持攻击取证，支持全流抓包(含三次握手信息)及攻击片段展示，方便运维；支持 X-Forwarded-For(XFF)字段提取。 说明：IPS6525F 支持 13,000+签名
反病毒	支持 HTTP/FTP/SMTP/POP3/IMAP4/NFS/SMB 等协议的文件病毒检测； 可检测支持木马、蠕虫、间谍软件、漏洞利用程序、广告软件、黑客工具、Rootkit、后门、灰色软件、僵尸网络程序、勒索软件、钓鱼软件、挖矿软件、勒索软件、Web shell 程序等检测，支持 Office 文档类型、可执行文件（Windows/Linux/MacOS）、脚本文件、Flash 文件、PDF 文件、RTF 文件、网页、图片等各种文件类型病毒检测；支持攻击取证；支持 tar/gzip/zip/rar/7z 等多种压缩混合及多层压缩检测，最大支持 100 层压缩文件病毒检测。
基于 AI 的恶意软件防护	反病毒引擎非基于威胁信息/信誉的检测，采用启发式/AI/语义分析等检测技术，可支持加壳病毒检测，脚本变形检测，复合文档内嵌病毒检测；覆盖亿级变种病毒检测，并支持特征库自动升级。
Web 安全上网	支持Web/URL过滤，支持基于新闻/游戏/赌博/毒品/恶意网页等130+的分类能力，云端分类库超过5.6亿；URL云端分类查询服务器全球部署，提供高速度、低时延的分类查询服务，同时满足不同国家/地区的管理要求；支持自定义URL/Host黑白名单过滤；支持HTTPS不解密过滤；支持TLS/SSL解密过滤，支持HTTP/2过滤；支持批量导入恶意分类URL。
DNS 安全	支持联动云端进行DNS恶意域名过滤 支持DNS恶意域名的防护，包括Command-and-Control，DGA，失陷站点，挖矿、勒索、钓鱼等恶意域名的过滤，本地最大支持200万的DNS恶意域名库。
防僵尸网络	支持僵尸网络恶意程序的检测，支持僵尸网络软件恶意流量的检测，包括签名检测和威胁信息检测，支持僵尸网络攻击日志中通信双方在僵尸网络角色信息显示。支持基于AI的加密流量检测技术（ECA），支持C&C流量检测。

模型藏毒检测	基于模型文件内容极速检测，支持onnx/pickle/safetensors/pth/checkpointh等主流模型文件，防护恶意模型加载引发资产窃取和破坏。
提示词攻击防护	支持通过静态规则或自定义正则规则对模型输入内容进行过滤，支持采用语义分析和AI技术对提示词攻击模式进行识别，防止SQL注入、XSS和RCE等注入攻击。
Anti-DDoS	支持针对DDoS攻击和单包攻击的防御，防范SYN Flood、UDP Flood、ICMP Flood、HTTP Flood、HTTPS Flood、DNS Flood和SIP Flood等10+种常见DDoS攻击以及20+种单包攻击。
IPv6 报文检测	支持 IPv4/IPv6 双栈，支持 IPv6 报文检测及防护。
隧道报文检测	支持 VLAN、GRE、IPv4 over IPv6、IPv6 over IPv4 等隧道报文检测。
响应方式	日志告警、丢弃报文、阻断、限流。
带宽管理	在识别业务应用的基础上，可管理每用户/IP 使用的带宽，确保关键业务和关键用户的网络体验。 管控方式包括：限制最大带宽或保障最小带宽、修改应用转发优先级等。
日志报表	可视化多维度报表呈现，支持 IP 地址、应用、时间、流量、威胁等多维度呈现报表。
工控安全	支持工控应用协议管控，减少已知漏洞入侵风险，详细支持的工控协议种类查询网址： https://isecurity.huawei.com/security/home 选择安全百科-应用识别百科-商务系统-工业应用。
升级	支持在线自动及手动升级、离线升级、集中升级，热补丁升级。
系统配置管理和维护	支持 GUI 图形化配置和命令行配置，支持远程管理和集中管理，提供独立的管理接口； 管理员分权分域，支持本地安全认证、服务器认证等多种认证方式； 支持诊断功能和系统资源管理。
部署方式及工作模式	支持接口对直路部署、旁路检测部署、直路/旁路混合部署； 支持二、三层基本转发，支持静态路由及动态路由协议。
部署及可靠性	透明、路由、混合部署模式，支持主/主、主/备 HA 特性。

6 订购信息

产品	型号	描述
IPS6525F	IPS6525F-AC	IPS6525F 交流主机(16*GE RJ45 + 12*GE SFP + 4*10GE SFP+ ,1 交流电源)
IPS6585F	IPS6585F-AC	IPS6585F 交流主机(8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+, 1 交流电源)
IPS6615F	IPS6615F-AC	IPS6615F 交流主机(8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+，1 交流电源)
IPS6625F	IPS6625F-AC	IPS6625F 交流主机(8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+，2 交流电源)

IPS6655F	IPS6655F-AC	IPS6655F 交流主机(4*QSFP28 + 16*ZSFP+ + 8*SFP+ , 2 交流电源)
基本 License		
IPS 特征库升级服务	LIC-IPS6525F-IPS-1Y	IPS 特征库升级 12 个月(适用于 IPS6525F)
	LIC-IPS6585F-IPS-1Y	IPS 特征库升级 12 个月(适用于 IPS6585F)
	LIC-IPS6615F-IPS-1Y	IPS 特征库升级 12 个月(适用于 IPS6615F)
	LIC-IPS6615F-IPS-3Y	IPS 特征库升级 36 个月(适用于 IPS6515F)
	LIC-IPS6625F-IPS-1Y	IPS 特征库升级 12 个月(适用于 IPS6625F)
	LIC-IPS6655F-IPS-1Y	IPS 特征库升级 12 个月(适用于 IPS6655F)
AV 升级服务	LIC-IPS6525F-AV-1Y	AV 特征库升级 12 个月(适用于 IPS6525F)
	LIC-IPS6585F-AV-1Y	AV 特征库升级 12 个月(适用于 IPS6585F)
	LIC-IPS6615F-AV-1Y	AV 特征库升级 12 个月(适用于 IPS6615F)
	LIC-IPS6615F-AV-3Y	AV 特征库升级 36 个月(适用于 IPS6615F)
	LIC-IPS6625F-AV-1Y	AV 特征库升级 12 个月(适用于 IPS6625F)
	LIC-IPS6655F-AV-1Y	AV 特征库升级 12 个月(适用于 IPS6655F)
URL 升级服务	LIC-IPS6525F-URL-1Y	URL 远程查询升级 12 个月(适用于 IPS6525F)
	LIC-IPS6585F-URL-1Y	URL 远程查询升级 12 个月(适用于 IPS6585F)
	LIC-IPS6615F-URL-1Y	URL 远程查询升级 12 个月(适用于 IPS6615F)
	LIC-IPS6615F-URL-3Y	URL 远程查询升级 36 个月(适用于 IPS6615F)
	LIC-IPS6625F-URL-1Y	URL 远程查询升级 12 个月(适用于 IPS6625F)
	LIC-IPS6655F-URL-1Y	URL 远程查询升级 12 个月(适用于 IPS6655F)
威胁防护升级服务	LIC-IPS6525F-TP-1Y	威胁防护 12 个月(适用于 IPS6525F)
	LIC-IPS6585F-TP-1Y	威胁防护 12 个月(适用于 IPS6585F)
	LIC-IPS6585F-TP-3Y	威胁防护 36 个月(适用于 IPS6585F)
	LIC-IPS6615F-TP-1Y	威胁防护 12 个月(适用于 IPS6615F)
	LIC-IPS6615F-TP-3Y	威胁防护 36 个月(适用于 IPS6615F)
	LIC-IPS6625F-TP-1Y	威胁防护 12 个月(适用于 IPS6625F)
	LIC-IPS6655F-TP-1Y	威胁防护 12 个月(适用于 IPS6655F)
恶意流量 AI 检测升级服务	LIC-IPS6525F-MTAI	恶意流量 AI 检测升级每年(适用于 IPS6525F)
	LIC-IPS6585F-MTAI	恶意流量 AI 检测升级每年(适用于 IPS6585F)
	LIC-IPS6615F-MTAI	恶意流量 AI 检测升级每年(适用于 IPS6615F)
	LIC-IPS6625F-MTAI	恶意流量 AI 检测升级每年(适用于 IPS6625F)
	LIC-IPS6655F-MTAI	恶意流量 AI 检测升级每年(适用于 IPS6655F)
内容安全组合功能	LIC-IPS-F-CONTENT	内容安全组合功能（适用于 IPS-F)
云沙箱检测服务	LIC-IPS6525F-CS-1Y	云沙箱检测服务每年(适用于 IPS6525F)
	LIC-IPS6585F-CS-1Y	云沙箱检测服务每年(适用于 IPS6585F)
	LIC-IPS6615F-CS-1Y	云沙箱检测服务每年(适用于 IPS6615F)
	LIC-IPS6625F-CS-1Y	云沙箱检测服务每年(适用于 IPS6625F)
	LIC-IPS6655F-CS-1Y	云沙箱检测服务每年(适用于 IPS6655F)