HiSecEngine USG12000系列

华为HiSecEngine USG12000系列AI防火墙

数字化浪潮正在席卷全球。前所未有的广泛连接、爆炸增长的数据以及蓬勃发展的智能应用将深刻改变人类的生活和工作方式。个人之间、个人和企业之间以及企业之间的交互会前所未有的频繁，各类数据交换并产生出的化学反应将会极大地推动经济和社会的发展。

在云计算、大数据技术的广泛应用下，企业数字化转型更加迅速。业务的智能化升级推动着企业网络的变革，同时为网络安全带来了更大的挑战。不法分子一直在尝试窃取个人隐私、企业机密乃至计算资源。我们在享受着数字化浪潮带来的便利，也不得不面对与之伴生的安全风险。未知威胁日益增多，并不断衍生出变种，让基于签名进行威胁检测的传统防火墙难以有效应对。随着 5G和IoT的发展，攻击变得更加立体，内网攻击不断增多，攻击面变得更宽。因此，在云服务提供商、大型数据中心和大型企业园区网络边界，迫切需要引入新一代的防火墙设备，应对不断变化的新型威胁，防患于未然。

HiSecEngine USG12004

HiSecEngine USG12008

HUAWEI

01 产品亮点

卓越性能

HiSecEngine USG12000系列AI防火墙使用全新软硬件架构，通过自适应安全引擎（ASE）为业务模块动态分配资源，最大限度提高资源利用率，提升整体业务性能；同时针对核心业务，使用NP（Network Prosessor）、模式匹配、加解密协处理引擎，有效提升小包转发性能、降低转发时延，增强应用识别和入侵防御检测以及IPSec等业务性能。

智能防御

- 签名1:N恶意文件家族
- 检测速度与签名检测性能相当
- 具有未知威胁检测能力

HiSecEngine USG12000系列AI防火墙提供应用识别、入侵防御（IPS）、反病毒和URL过滤等内容安全相关的功能，有效保证内网服务器和用户免受威胁的侵害。

传统IPS签名生产使用人工分析制作的方式，生产效率低，签名的准确度对专家经验的依赖度高。华为创新使用智能技术+专家经验赋能采用智能云端入侵防御签名生产的方式，签名生产率较人工提升30倍，同时降低人工分析带入的误差，持续提升入侵检测的准确度。

内置支持基于智能技术的防病毒内容检测引擎（CDE）覆盖亿级病毒样本，结合AI安全检测模型，通过对病毒进行深度分析，快速检测恶意文件、勒索软件等，有效提高威胁检出率。

极简运维

HiSecEngine USG12000系列提供全新的Web UI界面，以威胁可视化定义新安全界面，直观呈现设备状态、告警、流量、威胁事件等关键信息，实现多维数据钻取，关注客户的使用体验，不断改进易用性，简化运维。

02 产品说明

华为HiSecEngine USG12000系列AI防火墙，是业界首个T级AI防火墙系列。华为HiSecEngine USG12000系列产品包括USG12004和USG12008两款产品，提供业界领先的安全防护性能和扩展能力。

HiSecEngine USG12000系列采用了华为自研多核处理芯片以及分布式硬件平台，提供业界领先业务处理能力和业务扩展能力。所有部件均采用全冗余技术，使得设备达到核心路由器级别的高可靠性，从而保证高速网络环境下的业务连续性。

HiSecEngine USG12000系列提供多种接口模块（LPU）负责对外连接和数据传递。接口模块和业务处理模块采用相同的接口插槽，可通过不同接口模块和业务处理模块的组合，匹配用户网络对接口和性能的组合需求，量身定制安全防护方案。可以支持GE接口、10GE接口、40GE接口、100GE接口和400GE接口，可灵活适应大接口容量或高接口密度等不同的应用场景需求。

HiSecEngine USG12000业务处理模块（SPCD）负责处理所有的业务。SPCD子卡分为防火墙业务处理子卡和威胁防护处理子卡，可灵活组合不同性能单板。采用多核多处理器硬件，通过软件模块实现各种业务特性。

03 产品规格

参数 \ 型号	HiSecEngine USG12004	HiSecEngine USG12008
扩展及I/O		
接口类型	支持 GE，10GE，40GE，100GE，400GE等接口	
业务板	防火墙业务板、威胁防护业务板	
可扩展业务槽位	4	8
尺寸、电源、运行环境		
尺寸 (W x D x H:mm)	442 x 874x 438（9.8U）	442 x 874 x 703(15.8U)
重量	空机箱 82.8kg，直流 满配 144.7kg，直流 空机箱 77.8kg，交流 满配 140.9kg，交流	空机箱 134.4kg，直流 满配 248.3kg，直流 空机箱 129.2kg，交流 满配 244.3kg，交流
电源AC	176VAC~290VAC；额定 220VAC	
高压直流(HVDC)	188V~288V/260V-400V；额定 240V/380V	
风道	前后风道	
工作环境温度	长期：0°C 至 40°C 存储：-40°C 至 70°C	
环境湿度	长期：5%RH ~ 85%RH，无凝结	

注：性能数据是在理想环境下测试得出，实际情况会因现网情况不同而出现变化。

04 安全特性

特性	描述
一体化防护	集传统防火墙、VPN、入侵防御、防病毒、带宽管理、Anti-DDoS、URL过滤等多种功能于一身，全局配置视图和一体化策略管理。
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，支持应用细分；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。
安全策略管理	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。支持策略自学习，可对命中的安全策略下的流量聚合，生成子安全策略，实现细分安全策略和精准的流量安全管理。 预置常用防护场景模板，快速部署安全策略，降低学习成本。可与第三方策略管理软件(FireMon，Algosec)对接，方便用户安全运维。
带宽管理	在识别业务应用的基础上，可管理每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。
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(含Windows、Unix/Linux等系统漏洞，数据库、Apache、IIS、Tomcat等软件及中间件漏洞)防护、Web攻击 (如SQL注入、XSS、RCE等)防护、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。
WAF	采用签名、语义分析、机器学习等技术，支持对SQL注入、跨站脚本攻击、RCE、CSRF、反序列化等OWASP Top 10攻击的检测，支持盗链保护、网页防篡改；支持HTTP方法及字段长度控制等。
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，支持告警、阻断、添加宣告、删除附件等多种响应动作。
高级恶意软件防护	反病毒引擎采用启发式、AI-Based、语义分析、Emulator等检测技术, 辅助情报/信誉等检测, 通过动态模拟沙箱执行，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；覆盖数十亿级变种病毒检测，并支持特征库自动升级。同时支持联动沙箱，把可疑文件送到沙箱进行进一步的检测，可检测更多的零日恶意软件。
Web安全	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, 支持20+语言, 重点分类支持100+语言；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及QUIC过滤; 支持批量导入恶意分类URL。 支持安全搜索：支持5大知名搜索引擎: YouTube, Bing, Google, Yahoo, Yandex. 强制过滤搜索结果中的不合法内容。 可以根据不同的用户/组、时间段和安全区域等信息，对用户/组进行URL访问控制，达到精确管理用户上网行为的目的。

特性	描述
DNS安全	支持DNS恶意域名过滤, 基于海量的威胁信息, 利用AI/知识图谱等技术发现恶意DNS请求，包括C&C（Command-and-Control）、DGA(Domain Generation Algorithm)、失陷站点、挖矿、勒索、钓鱼等恶意域名, 支持本地和联动华为安全中心云端实时检测。 同时还可以支持基于DNS的分类过滤, 支持DNS安全搜索、支持DNS重定向(Sinkhole)。
反僵尸网络/间谍软件	支持僵尸网络、木马、蠕虫、远控工具、间谍软件等恶意程序软件及相关恶意流量的检测, 对恶意软件进行反病毒和高级恶意软件防护检测, 阻止恶意程序下载; 对于恶意软件产生的恶意流量, 进行基于签名的检测，支持C&C流量检测，并可基于IP、恶意域名信誉快速检测；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。
威胁信息	基于华为安全智能中心，通过多AI算法及专家分析，每日生产海量的IP、域名、URL、文件等威胁信息；并通过自动升级同步这些威胁信息到设备进行威胁检测，快速阻断新型攻击；同时支持和第三方的威胁信息源对接，丰富检测规则。
OT/IoT安全	支持Modbus、S7、Profinet、OPC等常见工控协议和摄像头等物联网设备的识别和控制。支持摄像头等IoT设备、ICS/SCADA等工控软件和协议的漏洞检测。
Anti-DDoS	采用源IP探测、指纹检测、动态限流等技术，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，支持流量基线自学习，支持IP信誉过滤。
邮件过滤	支持邮件地址、实时黑名单列表、MIME邮件头字段（收发件人，主题等）过滤，支持SMTP发送邮件限速。
数据泄漏防护	支持100+真实文件类型识别，支持自定义文件后缀，并基于文件类型进行上传/下载传输分别控制；支持office文档、网页、代码、TXT等文件的关键字内容过滤，可自定义关键字、支持正则及权重配置。
SaaS访问控制	支持基于特征的SaaS应用识别和访问控制，并基于SaaS应用进行选路, 保证员工SaaS应用使用体验。
行为审计	支持对用户常见的上网行为进行审计, 规范用户上网, 包括FTP(上传/下载/命令等)、HTTP(发帖/搜索/浏览等)、DNS、Telnet、SNMP、邮件收发等行为的记录。
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。
业务智能选路	支持基于业务和地理位置的策略路由，在多出口场景下可根据多种负载均衡算法（如带宽比例、链路健康状态等）进行智能选路。
VPN加密	支持丰富高可靠性的VPN特性，如IPSec VPN、SSL VPN、GRE等；支持DES、3DES、AES、SHA、SM2/SM3/SM4等多种加密算法。
SSL加密流量检测	检测并防御隐藏在TLS/SSL加密流量中的威胁，可对TLS/SSL流量解密后进行入侵防御、反病毒、内容过滤、URL过滤等应用层防护，支持基于URL分类的白名单例外。
SSL卸载	替代服务器实现SSL加解密，有效降低服务器负载，并实现HTTP流量的负载均衡。
丰富的报表	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。 支持报表查看，包括流量报表、威胁报表、邮件过滤报表、带宽管理报表、系统报表、命中策略报表、文件过滤报表、内容过滤报表、URL报表，支持报表定制与订阅。
安全虚拟化	支持多种安全业务的虚拟化，包括防火墙、入侵防御、反病毒、VPN等。不同用户可在同一台物理设备上进行隔离的个性化管理。
路由特性	全面支持IPV4/IPV6下的多种路由协议，如RIP、OSPF、BGP、IS-IS、RIPng、OSPFv3、BGP4+、IPv6 IS-IS等。
IP组播	支持IPv4三层组播协议，如：IGMP、MSDP、PIM，提供点对多点的服务模式，降低带宽消耗。
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。
服务器负载均衡	全面支持IPv6，支持L4/L7层服务器负载分担，支持基于源IP、HTTP Cookie等多种会话保持方法；支持SSL卸载和加密；服务和安全策略结合，有效提升服务的安全性；支持基于多种协议如TCP、Radius、DNS、HTTP的健康检查用于及时感知服务器状态变化。
SRv6	支持IS-IS for SRv6、BGP for SRv6、SRv6 BE、SRv6 TE Policy、SRv6中间节点保护、SRv6防微环、SRv6 OAM、SRv6 SRH压缩、SRv6 TI-LFA FRR、EVPN L3VPN。
用户认证	上网用户支持多种用户认证方式，包括本地Portal认证和单点登录。本地Portal认证支持推送设备内置的Portal页面，并将上网用户在Portal页面输入的账号密码推送到本地数据库或RADIUS、HWTACACS、AD、LDAP认证服务器进行认证。单点登录包含RADIUS单点登录和Agile Controller（NCE-Campus）单点登录两种方式。
运维能力	支持telemetry，自动读取硬件（风扇/电源/光模块/以太端口等）、温度传感器、驱动信息，设备主动向采集器上送设备的接口流量统计、CPU和内存使用率。
PPPoE	支持作为PPPoE客户端提供上网服务，包括用户的认证授权，动态IP地址分配的能力。
SSL VPN支持Posture合规检查	支持操作系统版本检查、操作系统补丁检查、杀毒软件检查、防火墙检查、运行进程检查、文件安全检查、注册表检查、端口检查、防截屏、防二次跳转。

上述列举特性在HiSecEngine USG12000系列产品中根据具体版本支持程度略有不同。具体信息请咨询华为工程师。

05 订购信息

- 说明：为方便展示，以下均采用设备简称

主机	
USG12004-AC-B04	USG12004交流基本配置(含交流机箱,2*MPUD,2*交流电源,满配风扇)
USG12004-DC-B04	USG12004直流基本配置(含直流机箱,2*MPUD,2*直流电源,满配风扇)
USG12008-AC-B04	USG12008交流基本配置(含交流机箱,2*MPUD,4*SFUA,2*交流电源,满配风扇)
USG12008-DC-B04	USG12008直流基本配置(含直流机箱,2*MPUD,4*SFUA,2*直流电源,满配风扇)
USG12000业务处理板和接口板	
SFUA-USG12008	USG12008交换网板单元
SPUD-USG	USG12000防火墙业务处理底板D
SPCD-USG-02	USG12000防火墙业务处理子卡D-02
SPCD-USG-04	USG12000防火墙业务处理子卡D-04
SPCD-USG-TP-02	USG12000威胁防护业务处理子卡D-02
SPCD-USG-TP-04	USG12000威胁防护业务处理子卡D-04
LPUA-4CQ-24XS	24端口10GBase SFP+ + 4端口100GBase-QSFP接口板
LPUA-2CQ-24XS	24端口10GBase SFP+ + 2端口100GBase-QSFP接口板
LPUA-48XS	48端口10GBase SFP+接口板
LPUA-18CQ	18端口100GBase-QSFP+接口板
LPUA-4DQ	4端口400GE接口板
LPUA-12CQ24XS	12端口100GBase-QSFP28+24端口10GBase-SFP+接口板
软件	
LIC-USG12000-SSLVPN-100	SSL VPN并发用户数(100个)
LIC-USG12000-SSLVPN-200	SSL VPN并发用户数(200个)
LIC-USG12000-SSLVPN-500	SSL VPN并发用户数(500个)
LIC-USG12000-SSLVPN-1000	SSL VPN并发用户数(1000个)
LIC-USG12000-SSLVPN-2000	SSL VPN并发用户数(2000个)
LIC-USG12000-SSLVPN-5000	SSL VPN并发用户数(5000个)
LIC-USG12004-IPS-1Y	IPS特征库升级(适用于USG12004)
LIC-USG12004-AV-1Y	AV特征库升级(适用于USG12004)
LIC-USG12004-URL-1Y	URL远程查询升级(适用于USG12004)
LIC-USG12004-IAU-1Y	IPS+AV+URL特征库升级服务License(适用于USG12004) （包含web应用防护功能）
LIC-USG12004-CS-1Y	云沙箱检测服务每年(适用于USG12004)
LIC-USG12004-ICS-1Y	工控安全每年(适用于USG12004)
LIC-USG12008-IPS-1Y	IPS特征库升级(适用于USG12008)
LIC-USG12008-AV-1Y	AV特征库升级(适用于USG12008)
LIC-USG12008-URL-1Y	URL远程查询升级(适用于USG12008)
LIC-USG12008-IAU-1Y	IPS+AV+URL特征库升级服务License(适用于USG12008) （包含web应用防护功能）
LIC-USG12008-CS-1Y	云沙箱检测服务每年(适用于USG12008)
LIC-USG12008-CS-1Y	工控安全每年(适用于USG12008)

注：以上订购信息只是产品部分部件信息，具体信息请联系当地华为工程师。

华为技术有限公司
地址：深圳市龙岗区坂田华为总部办公楼
邮编：518129
网址：www.huawei.com

版权所有 © 华为技术有限公司2025。保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

HUAWEI ,HUAWEI , 是华为技术有限公司商标或者注册商标，在本手册中以及本手册描述的产品中， 出现的其它商标，产品名称，服务名称以及公司名称，由其各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。